ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ТЕХНОЛОГІЯ ЗАХИСТУ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ ВІД DDOS-АТАК»

на здобуття освітнього ступеня магістра
зі спеціальності ____125 Кібербезпека_____
(код, найменування спеціальності)
освітньо-професійної програми _Інформаційна та кібернетична безпека_
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Роман КОВАЛЬЧУК

Виконав: здобувач вищої освіти групи БСДМ-62
КОВАЛЬЧУК Роман
(ПРІЗВИЩЕ, Ім'я)

Керівник: БОРСУКОВСЬКИЙ Юрій
к.т.н., доцент (ПРІЗВИЩЕ, Ім'я)

Рецензент: _____
(ПРІЗВИЩЕ, Ім'я)

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
“___”_____ 2023 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Ковальчуку Роману Сергійовичу
(прізвище, ім’я, по батькові)

1. Тема кваліфікаційної роботи:
«Технологія захисту інформаційної системи організації від DDoS-атак»
керівник кваліфікаційної роботи: БОРСУКОВСЬКИЙ Юрій, к.т.н., доцент,
(ПРІЗВИЩЕ, Ім’я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «19» жовтня 2023р. №145.

2. Строк подання студентом кваліфікаційної роботи: 15.12.2023 р.

3. Вихідні дані до кваліфікаційної роботи:
інформаційна система організації;
технологія захисту інформаційної системи організації від DDoS-атак;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Дослідження проблеми захисту інформаційної системи організації від DDoS-атак.
2. Методи та засоби захисту інформаційної системи організації від DDoS-атак.

3. Розроблення варіанта технології захисту інформаційної системи організації від DDoS-атак.

5. Перелік ілюстративного матеріалу:
Презентація PowerPoint

6. Дата видачі завдання 19.10.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми захисту інформаційної системи організації від DDoS-атак.	19.10.2023 р.	
2.	Аналіз наукової та технічної літератури з питань теми кваліфікаційної роботи.	22.10.2023 р.	
3.	Аналіз методів та засобів захисту інформаційної системи організації від DDoS-атак .	27.10. 2023р.	
4.	Технологія захисту інформаційної системи організації від DDoS-атак.	03.11.2023 р.	
5.	Розроблення рекомендацій щодо застосування технології захисту інформаційної системи організації від DDoS-атак.	15.11.2023 р.	
6.	Оформлення результатів дослідження.	26.11.2023 р.	
7.	Підготовка доповіді до захисту.	15.12.2023 р.	

Здобувач(ка) вищої освіти _____ Роман КОВАЛЬЧУК
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Юрій БОРСУКОВСЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Ковальчук Р.С. до захисту кваліфікаційної роботи
(прізвище та ініціали)

За спеціальністю 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)

на тему: «Технологія захисту інформаційної системи організації від DDoS-атак».

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Віталій САВЧЕНКО
(*підпис*) (*Ім'я, ПРІЗВИЩЕ*)

Висновок керівника кваліфікаційної роботи

Здобувач ***КОВАЛЬЧУК Роман*** обрав тему роботи, метою якої було дослідити зміст технології захисту інформаційної системи організації від DDoS-атак. Перелік використаних джерел свідчить про вміння здобувача розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***КОВАЛЬЧУК Роман*** показав гарну теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***КОВАЛЬЧУКА Романа*** на оцінку **«добре»** та присвоїти йому кваліфікацію магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Юрій БОРСУКОВСЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*
"____" _____ 2023 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач(ка) ***КОВАЛЬЧУК Роман.*** допускається до захисту даної роботи в Державній екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Галина ГАЙДУР
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача Ковальчука Романа
на тему: «Технологія захисту інформаційної системи організації від DDoS-атак».

Актуальність:

Актуальність захисту інформаційної системи організації від DDoS-атак обумовлена зростаючою кількістю таких атак та їхньою здатністю серйозно впливати на операційну діяльність, фінансове становище та репутацію будь-якої організації. У сучасному цифровому світі, де бізнес-операції, комунікації та послуги усе більше залежать від інтернет-технологій, надійний захист від DDoS-атак є критично важливим...

Позитивні сторони:

1. На основі проведеного аналізу, в роботі встановлено зміст проблеми захисту інформаційної системи організації від DDoS-атак .
2. Досліджено методи та засоби захисту інформаційної системи організації від DDoS-атак.
3. Запропоновано варіант технології захисту інформаційної системи організації від DDoS-атак на базі Cloudflare.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою магістерської роботи.

Недоліки:

1. У кваліфікаційній роботі бажано було б провести аналіз захисту інформаційної системи організації від DDoS-атак на прикладі конкретної організації.
2. Запропонований порядок застосування технології захисту інформаційної системи організації від DDoS-атак бажано було б показати на прикладі конкретної організації.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку «**добре»**, а здобувач **КОВАЛЬЧУК Роман** - присвоєння кваліфікації магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Рецензент: _____ _____

підпис *Ім'я, ПРІЗВИЩЕ*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи и на здобуття освітнього ступеня магістра: 64 сторінки, 27 рисунків, 15 джерел.

Об'єкт дослідження – процес захисту інформаційної системи організації від DDoS-атак.

Предмет дослідження – технологія захисту інформаційної системи організації від DDoS-атак.

Мета роботи – розробити варіанти технології захисту інформаційної системи організації від DDoS-атак та рекомендації щодо застосування технології.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу управління захисту інформаційної системи організації від DDoS-атак.

В роботі проведено аналіз проблеми захисту інформаційної системи організації від DDoS-атак на основі застосування політик пристроїв і користувачів корпоративних мереж. Проаналізовано існуючі технології захисту інформаційної системи організації від DDoS-атак.

Досліджено методи та засоби захисту інформаційної системи організації від DDoS-атак.

Запропоновано варіант технології захисту інформаційної системи організації від DDoS-атак. Визначено призначення, основні функції та склад компонентів даної технології.

На основі проведених досліджень, в роботі розроблено варіант технології захисту інформаційної системи організації від DDoS-атак для різної кількості користувачів організації

Галузь використання – кібербезпека корпоративної інформаційної системи.

ІНФОРМАЦІЙНА СИСТЕМА ОРГАНІЗАЦІЇ, КІБЕРБЕЗПЕКА, ЗАХИСТ ВІД DDOS-АТАК, МЕТОДИ ТА ЗАСОБИ, АРХІТЕКТУРА, МОДУЛІ, ФУНКЦІЇ

ABSTRACT

Text part of the master's qualification work: 64 pages, 27 figures, 15 sources.

Object of research - the process of protecting the organization's information system from DDoS attacks.

Subject of research - is the technology of protecting the organization's information system from DDoS attacks.

The aim of research – to develop options for technology to protect the organization's information system from DDoS attacks and recommendations for the use of technology.

Research methods - studying the literature on this topic, analysis of operational documentation, international standards and their comparison, modeling the process of managing the protection of an organization's information system from DDoS attacks.

The paper analyzes the problem of protecting an organization's information system from DDoS attacks based on the application of policies for devices and users of corporate networks. The existing technologies for protecting an organization's information system from DDoS attacks are analyzed.

The methods and means of protecting the organization's information system from DDoS attacks are investigated.

A variant of the technology for protecting the organization's information system from DDoS attacks is proposed. The purpose, main functions and composition of the components of this technology are determined.

Based on the research, a variant of the technology for protecting the organization's information system from DDoS attacks for a different number of users of the organization is developed in the work.

Scope - cybersecurity of a corporate information system.

ORGANIZATION'S INFORMATION SYSTEM, CYBERSECURITY, PROTECTION AGAINST DDOS-ATTACKS, METHODS AND MEANS, ARCHITECTURE, MODULES, FUNCTIONS

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

DDoS — Distributed Denial of Service

OSI — Open System Interconnection

HTTP — HyperText Transfer Protocol

URL — Uniform Resource Locator

TCP — Transmission Control Protocol

SYN-ACK — Synchronize-Acknowledge

DNS — Domain Name System

ISP — Internet Service Provider

WAF — Web Application Firewall

UDP — User Datagram Protocol

ACL — Access Control List

CDN — Content Delivery Network

ВСТУП

Актуальність дослідження. Актуальність захисту інформаційних систем організацій від DDoS-атак у сучасному цифровому світі є високою і продовжує зростати. У контексті збільшення залежності бізнесу від цифрових технологій, кібербезпека стає ключовим пріоритетом. DDoS-атаки, які характеризуються своєю спроможністю перевантажувати системи величезним обсягом трафіку, можуть призвести до серйозних наслідків, включаючи втрату доступності важливих онлайн-сервісів, фінансові втрати, а також пошкодження репутації.

У світлі постійної еволюції та зміцнення методів кібератак, організації повинні адаптувати свої стратегії безпеки, щоб адекватно захистити свої інформаційні системи. Це включає в себе впровадження комплексних рішень, таких як розширені системи виявлення та пом'якшення наслідків DDoS-атак, а також розробку планів реагування на інциденти та аварійного відновлення.

Окрім технологічних аспектів, важливим є також забезпечення навчання та обізнаності співробітників щодо потенційних загроз та кращих практик кібербезпеки. Ураховуючи постійну зміну кіберзагроз, постійний моніторинг та адаптація стратегій безпеки є необхідними для забезпечення надійного захисту інформаційних систем.

Об’єкт дослідження – процес захисту інформаційної системи організації від DDoS-атак.

Предмет дослідження – технологія захисту інформаційної системи організації від DDoS-атак.

Мета роботи – розробити варіанти технології захисту інформаційної системи організації від DDoS-атак та рекомендації щодо застосування технології.

Наукові завдання:

дослідити сутність проблеми забезпечення захисту інформаційної системи організації від DDoS-атак;

встановити сутність завдань захисту інформаційної системи організації від DDoS-атак;

проаналізувати існуючі технології захисту інформаційної системи організації від DDoS-атак;

проаналізувати методи та засоби забезпечення захисту інформаційної системи організації від DDoS-атак;

проаналізувати основні функції та принципи реалізації захисту інформаційної системи організації від DDoS-атак.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу управління захисту інформаційної системи організації від DDoS-атак.

Практичне значення одержаних результатів полягає в розробці варіанта технології захисту інформаційної системи організації від DDoS-атак на базі Cloudflare, а також у розробці рекомендацій щодо застосування технології захисту інформаційної системи організації від DDoS-атак.

Апробація результатів кваліфікаційної роботи було оприлюднено на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2023 року в Державному університетіінформаційнокомунікаційних технологій м. Київ.

1 АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ ВІД DDOS-АТАК

1.1. Аналіз проблеми забезпечення захисту інформаційної системи організації від DDoS-атак

Розподілена атака на відмову в обслуговуванні (DDoS-атака) - це зловмисна спроба порушити нормальну роботу сервера, служби або мережі, на яку спрямована атака, шляхом переповнення цільового сервера або навколишньої інфраструктури величезним потоком інтернет-трафіку.

Ефективність DDoS-атак досягається завдяки використанню декількох скомпрометованих комп'ютерних систем як джерел атакуючого трафіку. Експлуатовані машини можуть включати комп'ютери та інші мережеві ресурси, такі як пристрої Інтернету речей. З високого рівня, DDoS-атака схожа на несподіваний затор, який забиває шосе, не даючи звичайному транспорту прибути до місця призначення.

DDoS-атаки здійснюються за допомогою мереж машин, підключених до Інтернету. Ці мережі складаються з комп'ютерів та інших пристроїв (наприклад, пристроїв Інтернету речей), які були заражені шкідливим програмним забезпеченням, що дозволяє зловмиснику дистанційно керувати ними. Ці окремі пристрої називаються ботами (або зомбі), а група ботів - ботнетом.

Після створення ботнету зловмисник може керувати атакою, надсилаючи віддалені інструкції кожному боту.

Коли ботнет атакує сервер або мережу жертви, кожен бот надсилає запити на IP-адресу жертви, що може призвести до перевантаження сервера або мережі і, як наслідок, до відмови в обслуговуванні звичайного трафіку.

Оскільки кожен бот є легальним інтернет-пристроєм, відокремити атакуючий трафік від звичайного може бути складно.

Найочевиднішою ознакою DDoS-атаки є раптова повільна робота або недоступність сайту чи сервісу. Але оскільки подібні проблеми з продуктивністю можуть виникати з різних причин, наприклад, через природний сплеск трафіку, зазвичай потрібне подальше розслідування. Інструменти аналізу трафіку можуть допомогти виявити деякі з цих ознак DDoS-атаки:

- Підозрілі обсяги трафіку, що надходять з однієї IP-адреси або діапазону IP-адрес;
- Потік трафіку від користувачів, які мають спільний поведінковий профіль, наприклад, тип пристрою, геолокацію або версію веб-браузера;
- Незрозумілий сплеск запитів до однієї сторінки або кінцевої точки;
- Дивні моделі трафіку, такі як сплески в непарні години дня або моделі, які виглядають неприродно (наприклад, сплеск кожні 10 хвилин).

Існують й інші, більш специфічні ознаки DDoS-атаки, які можуть відрізнятися залежно від типу атаки [1].

1.2. Типи DDoS-атак, використання та функції ботнету, процес пом'якшення наслідків DDoS-атаки

Різні типи DDoS-атак націлені на різні компоненти мережевого з'єднання. Для того, щоб зрозуміти, як працюють різні DDoS-атаки, необхідно знати, як створюється мережеве з'єднання.

Мережеве з'єднання в Інтернеті складається з багатьох різних компонентів або "шарів". Як і при будівництві будинку з нуля, кожен рівень в моделі має своє призначення.

Модель OSI, показана нижче, є концептуальною основою, яка використовується для опису мережевого з'єднання на 7 різних рівнях.

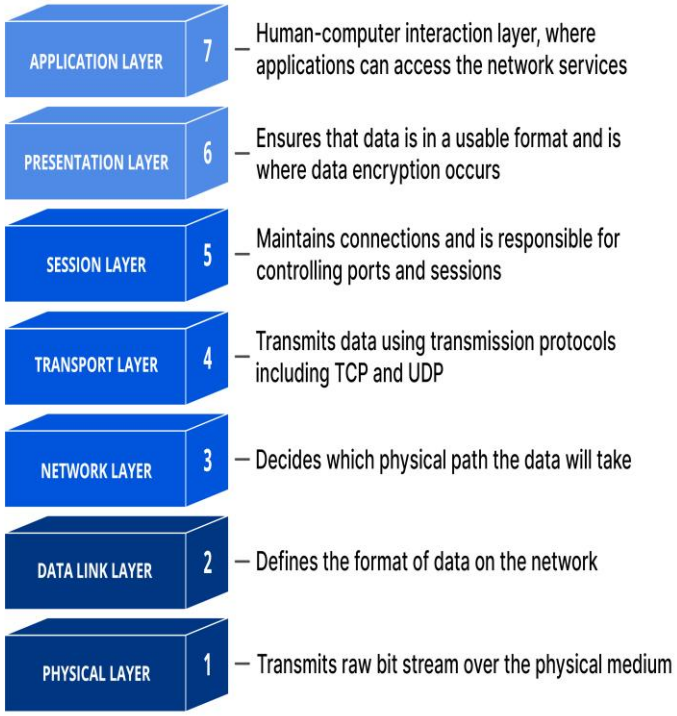

Рис. 1.1. Модель OSI, яка використовується для опису мережевого з'єднання

Хоча майже всі DDoS-атаки пов'язані з перевантаженням цільового пристрою або мережі трафіком, атаки можна розділити на три категорії. Зловмисник може використовувати один або кілька різних векторів атаки, або циклічно змінювати вектори атаки у відповідь на контрзаходи, які вживає ціль.

Атаки на прикладному рівні

Мета атаки:

Іноді їх називають DDoS-атаками 7-го рівня (посилаючись на 7-й рівень моделі OSI), метою цих атак є виснаження ресурсів цілі для створення відмови в обслуговуванні.

Атаки націлені на рівень, де веб-сторінки генеруються на сервері і доставляються у відповідь на HTTP-запити. Один HTTP-запит є дешевим в обчислювальному плані для виконання на стороні клієнта, але відповідь на нього може бути дорогою для сервера-мішені, оскільки сервер часто

завантажує кілька файлів і виконує запити до бази даних, щоб створити веб-сторінку.

Від атак 7-го рівня важко захиститися, оскільки буває важко відрізнити зловмисний трафік від легітимного.

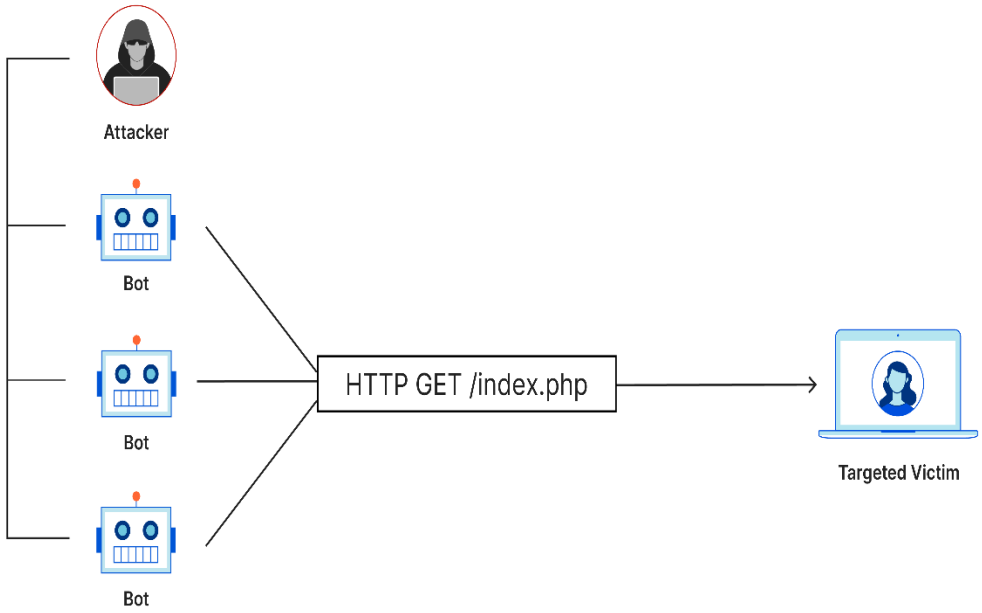

Рис. 1.2. Приклад атаки на прикладному рівні

HTTP-флуд

Ця атака схожа на натискання кнопки "Оновити" у веб-браузері знову і знову на багатьох різних комп'ютерах одночасно - велика кількість HTTP-запитів переповнює сервер, що призводить до відмови в обслуговуванні.

Цей тип атаки варіюється від простого до складного.

Прості реалізації можуть отримати доступ до однієї URL-адреси з одним і тим же діапазоном атакуючих IP-адрес, реферерів і агентів користувачів. Складні версії можуть використовувати велику кількість атакуючих IP-адрес і націлюватися на випадкові URL-адреси, використовуючи випадкових реферерів і агентів користувачів.

Атаки на протокол

Мета атаки:

Протокольні атаки, також відомі як атаки на виснаження стану, спричиняють збій у роботі сервісу шляхом надмірного споживання ресурсів сервера та/або мережевого обладнання, такого як брандмауери та балансувальники навантаження.

Протокольні атаки використовують слабкі місця на 3-му та 4-му рівнях стеку протоколів, щоб зробити ціль недоступною.

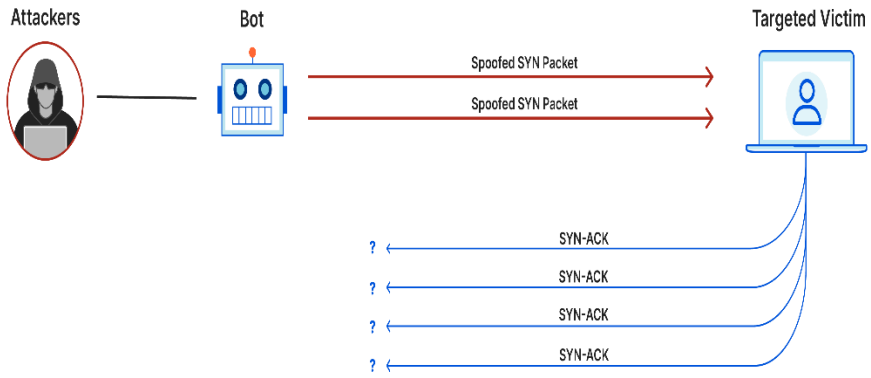

Рис. 1.3. Приклад атаки на протокол

SYN-флуд

SYN Flood є типом DDoS (Distributed Denial of Service) атаки, що використовує принципи TCP (Transmission Control Protocol) для перевантаження цільової системи. У нормальному TCP-з'єднанні, процес встановлення зв'язку між клієнтом та сервером відбувається за трьома етапами, відомими як TCP 3-way handshake:

1. Клієнт відправляє SYN (synchronize) пакет на сервер, щоб розпочати з'єднання.

2. Сервер відповідає SYN-ACK (synchronize-acknowledge) пакетом, підтверджуючи отримання SYN і відправляючи свій власний SYN запит.
3. Клієнт відсилає ACK (acknowledge) пакет для підтвердження SYN-ACK від сервера, завершуючи процес установки зв'язку.

Під час SYN Flood атаки, зловмисник відправляє безліч SYN пакетів на цільовий сервер, але навмисно не завершує процес установки зв'язку, ігноруючи або фальсифікуючи відправку ACK пакетів. Це призводить до того, що сервер очікує на завершення кожного з цих підвішених з'єднань, що використовує його ресурси та може заповнити весь доступний пул для нових з'єднань. У результаті законні користувачі не можуть встановити зв'язок з сервером, оскільки він перевантажений фальшивими запитами.

Об'ємні атаки

Мета атаки:

Ця категорія атак намагається створити перевантаження, споживаючи всю доступну пропускну здатність між мішенню і Інтернетом. Великі обсяги даних надсилаються на ціль за допомогою ампліфікації або іншого способу створення масового трафіку, наприклад, запитів від ботнету.

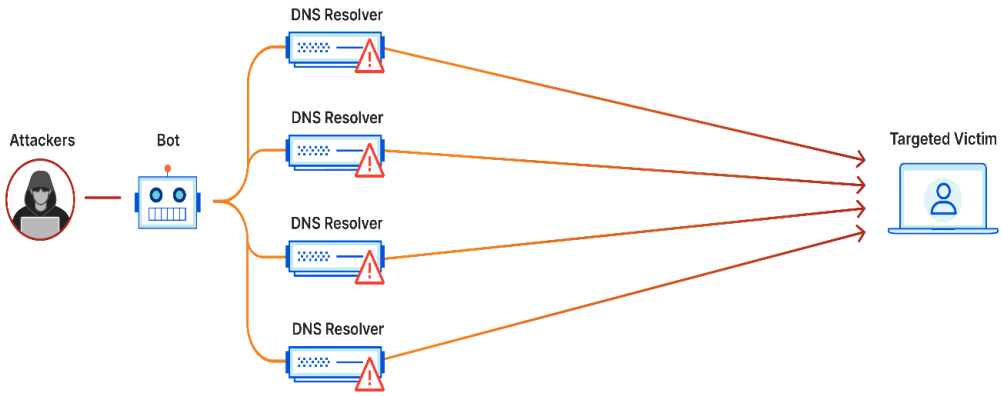

Рис. 1.4. Приклад ампліфікації

Підсилення DNS

DNS-ампліфікація є типом розподіленої атаки відмови у обслуговуванні (DDoS), яка використовує особливості DNS (Domain Name System) для підсилення обсягу атаки. Основна стратегія цього типу атаки полягає в надсиланні невеликих запитів до DNS-серверів з підробленою (фальсифікованою) IP-адресою жертви так, що відповідь на ці запити надсилається не зловмиснику, а цільовій системі.

Процес атаки включає наступні етапи:

1. Ініціювання Запиту: Зловмисник відправляє запити до різних DNS-серверів, використовуючи IP-адресу жертви як відправника запиту.
2. Підроблення IP-Адреси: У запитах DNS, IP-адреса "відправника" підроблена, так що відповіді від серверів надсилаються не атакуючому комп'ютеру, а цільовій системі (жертві).
3. Ампліфікація: Важливою особливістю атаки є те, що розмір відповіді DNS значно більший за розмір запиту. Тобто невеликі запити генерують значно більші відповіді.
4. Перевантаження Цільової Системи: Великий обсяг відповідей DNS з великою кількістю даних надсилається на цільову систему (жертву), що може призвести до перевантаження її мережевих ресурсів та викликати відмову в обслуговуванні для легітимного трафіку.

DNS-ампліфікація є особливо ефективною, оскільки вона дозволяє атакуючим генерувати значний обсяг мережевого трафіку, використовуючи лише невелику кількість ініційованих запитів. Це робить її популярним методом серед зловмисників для проведення DDoS-атак.

Ботнет

Ботнет - це група комп'ютерів, які були заражені шкідливим програмним забезпеченням і перейшли під контроль зловмисника. Термін "ботнет" - це калька зі слів "робот" і "мережа", а кожен заражений пристрій називається "ботом". Ботнети можуть бути призначені для виконання незаконних або шкідливих завдань, включаючи розсилку спаму, крадіжку

даних, вимагання викупу, шахрайські кліки на рекламу або розподілені атаки типу "відмова в обслуговуванні" (DDoS).

У той час як деякі шкідливі програми, такі як програми-вимагачі, безпосередньо впливають на власника пристрою, шкідливі програми DDoS-бот-мереж можуть мати різні рівні видимості; деякі шкідливі програми призначені для повного контролю над пристроєм, тоді як інші працюють безшумно як фоновий процес, мовчки чекаючи інструкцій від зловмисника або "пастуха ботів".

Ботнети, що саморозповсюджуються, вербують додаткових ботів через безліч різних каналів. Шляхи зараження включають використання вразливостей веб-сайтів, шкідливого програмного забезпечення типу "троянський кінь" і злом слабкої автентифікації для отримання віддаленого доступу. Після отримання доступу всі ці методи зараження призводять до встановлення шкідливого програмного забезпечення на цільовий пристрій, що дозволяє оператору ботнету віддалено керувати ним. Після зараження пристрій може намагатися самостійно поширювати шкідливе програмне забезпечення ботнету, залучаючи до нього інші апаратні пристрої в навколишній мережі.

Хоча неможливо визначити точну кількість ботів у конкретному бот-мережі, за оцінками, загальна кількість ботів у складних ботнетах коливається від кількох тисяч до понад мільйона.

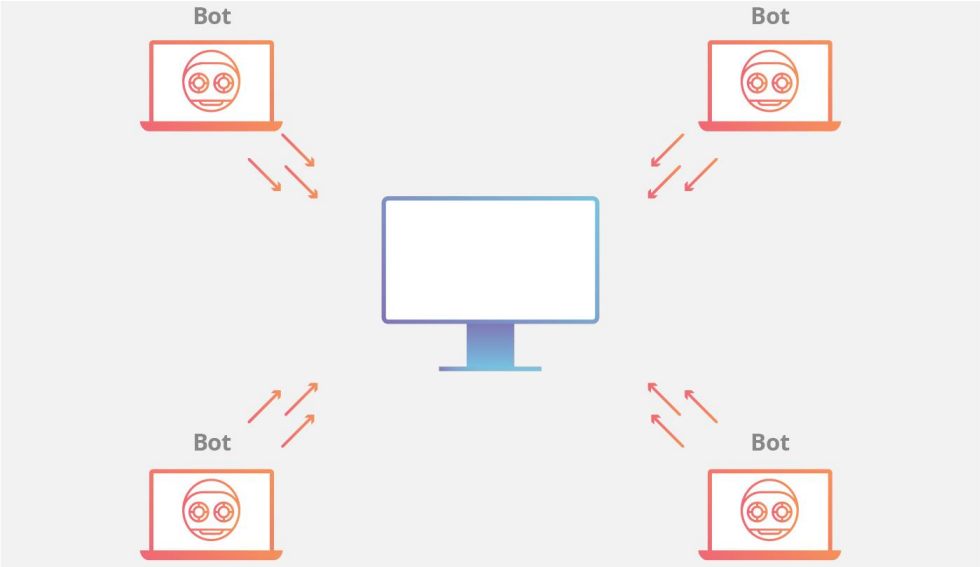

Рис. 1.5. Принцип роботи DDoS-бот-мереж

Причини використання бот-мереж варіюються від активізму до підриву діяльності держави, причому багато атак здійснюються просто з метою отримання прибутку. Найняти послуги ботнету в Інтернеті відносно недорого, особливо в порівнянні з обсягом шкоди, яку вони можуть завдати. Бар'єр для створення ботнету також досить низький, щоб зробити його прибутковим бізнесом для деяких розробників програмного забезпечення, особливо в географічних регіонах, де регулювання і правоохоронна діяльність обмежені. Ця комбінація призвела до поширення онлайн-сервісів, що пропонують атаки на замовлення.

Основною характеристикою бот-мережі є можливість отримувати оновлені інструкції від пастуха ботів. Можливість спілкуватися з кожним ботом у мережі дозволяє зловмиснику змінювати вектори атаки, змінювати цільову IP-адресу, припиняти атаку та здійснювати інші індивідуальні дії. Дизайн бот-мереж може бути різним, але структури управління можна розбити на дві основні категорії:

- Модель ботнету клієнт/сервер

Модель клієнт/сервер імітує традиційний робочий процес віддаленої робочої станції, де кожна окрема машина підключається до централізованого сервера (або невеликої кількості централізованих серверів), щоб отримати

доступ до інформації. У цій моделі кожен бот підключається до ресурсу командно-контрольного центру (КЦ), такого як веб-домен або IRC-канал, щоб отримувати інструкції. Використовуючи ці централізовані сховища для надання нових команд для ботнету, зловмиснику потрібно лише змінити вихідний матеріал, який кожен бот отримує з командного центру, щоб оновити інструкції для заражених машин. Централізований сервер, який контролює ботнет, може бути пристроєм, що належить зловмиснику, або ж зараженим пристроєм.

До популярних топологій централізованих бот-мереж відносяться:

- Топологія «зірка»
- Багатосерверна топологія мережі
- Ієрархічна топологія мережі

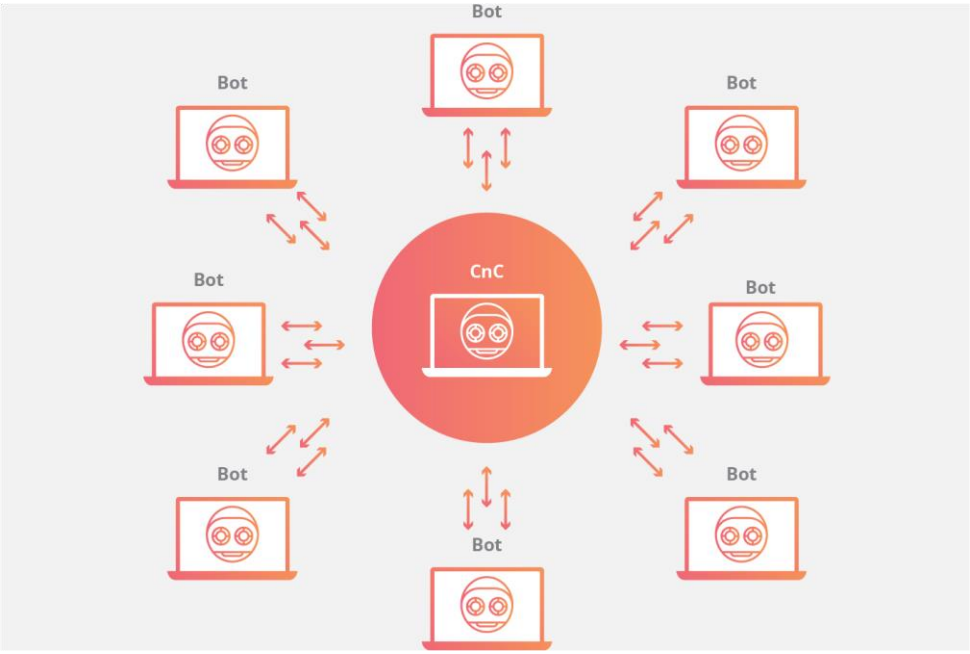

Рис. 1.6. Топологія «зірка»

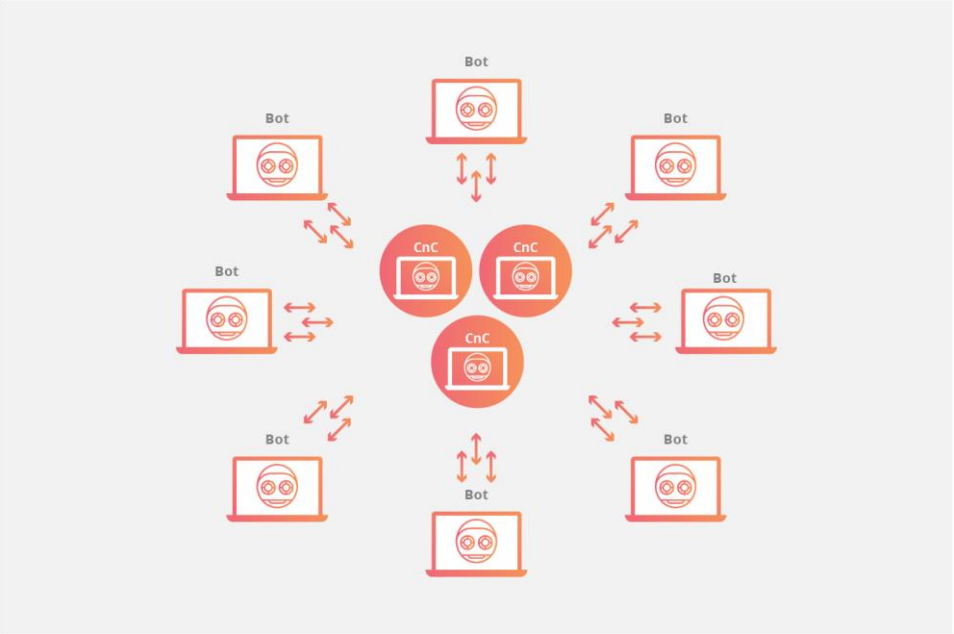

Рис. 1.7. Багатосерверна топологія мережі

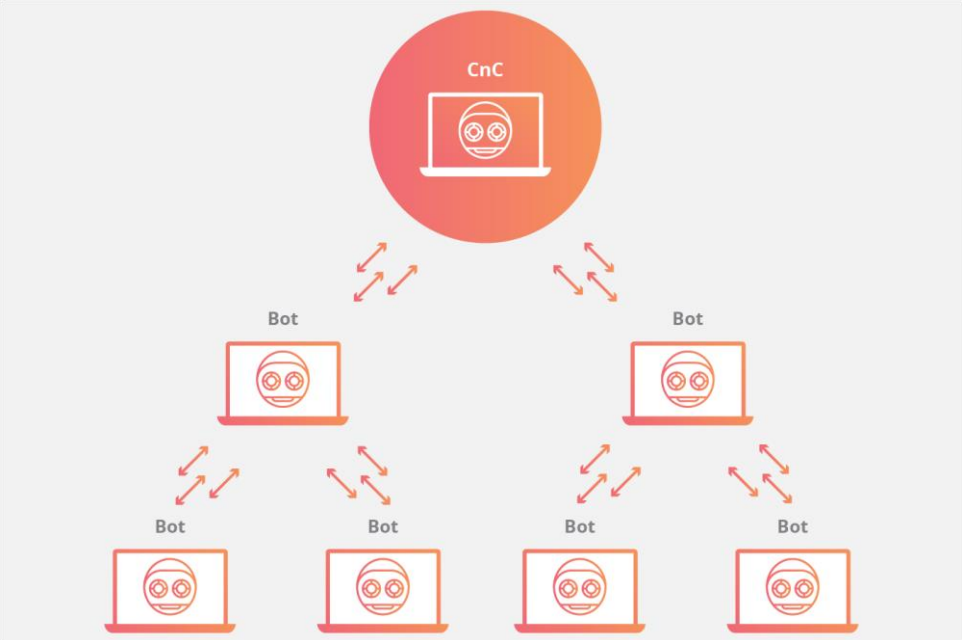

Рис. 1.8. Ієрархічна топологія мережі

У будь-якій з цих клієнт-серверних моделей кожен бот підключається до ресурсу командного центру, такого як веб-домен або IRC-канал, щоб отримати інструкції. Використовуючи ці централізовані репозиторії для надання нових команд для ботнету, зловмиснику достатньо змінити вихідний

матеріал, який кожен бот отримує з командного центру, щоб оновити інструкції для заражених машин.

Одночасно з простотою оновлення інструкцій для ботнету з обмеженої кількості централізованих джерел існує і вразливість цих машин: щоб видалити ботнет з централізованим сервером, потрібно вивести з ладу лише сам сервер. В результаті цієї вразливості творці шкідливого програмного забезпечення для бот-мереж еволюціонували і перейшли до нової моделі, яка є менш чутливою до виведення з ладу через одну або кілька точок відмови.

- Модель однорангового ботнету

Щоб обійти вразливості моделі клієнт/сервер, останнім часом ботнети розробляються з використанням компонентів децентралізованого однорангового файлообміну. Вбудовування структури управління всередину ботнету усуває єдину точку відмови, яка присутня в ботнетах з централізованим сервером, що ускладнює заходи з мінімізації ризиків. P2P-боти можуть бути як клієнтами, так і командними центрами, що працюють пліч-о-пліч зі своїми сусідніми вузлами для поширення даних. Вони ведуть список довірених комп'ютерів, з якими вони можуть обмінюватися даними і отримувати повідомлення, а також оновлювати своє шкідливе програмне забезпечення. Обмежуючи кількість інших комп'ютерів, до яких підключається бот, кожен бот піддається впливу лише сусідніх пристроїв, що ускладнює його відстеження та боротьбу зі шкідливим програмним забезпеченням. Відсутність централізованого командного сервера робить одноранговий ботнет більш вразливим до контролю з боку будь-кого, крім його творця. Для захисту від втрати контролю децентралізовані ботнети зазвичай шифруються, щоб обмежити доступ до них.

Принцип становлення ботнетом пристроїв Інтернету речей

Ніхто не користується інтернет-банкінгом через бездротову камеру відеоспостереження, яку поставив на задньому дворі, щоб спостерігати за годівницею для птахів, але це не означає, що пристрій не здатен робити необхідні мережеві запити. Потужність пристроїв Інтернету речей у

поєднанні зі слабкою або погано налаштованою системою безпеки створює можливість для шкідливого програмного забезпечення бот-мереж вербувати нових ботів до свого колективу. Зростання кількості пристроїв Інтернету речей призвело до появи нового ландшафту для DDoS-атак, оскільки багато пристроїв погано налаштовані та вразливі.

Якщо вразливість пристрою Інтернету речей закладена у прошивці, то оновлення ускладнюється. Щоб зменшити ризик, пристрої Інтернету речей із застарілою прошивкою слід оновлювати, оскільки облікові дані за замовчуванням зазвичай залишаються незмінними з моменту початкового встановлення пристрою. Багато виробників обладнання зі знижками не зацікавлені робити свої пристрої більш безпечними, тому вразливість, яку становлять шкідливі програми ботнетів для пристроїв Інтернету речей, залишається невирішеним ризиком безпеки [2].

Процес пом'якшення наслідків DDoS-атаки

Ключовим моментом у боротьбі з DDoS-атаками є розмежування трафіку, що атакує, та звичайного трафіку.

Наприклад, якщо після виходу нового продукту веб-сайт компанії завалений нетерплячими клієнтами, перекривати весь трафік буде помилкою.

Якщо ж раптом трафік компанії різко зростає від відомих зловмисників, то, ймовірно, необхідно вжити заходів, щоб послабити атаку.

Складність полягає в тому, щоб відрізнити справжніх клієнтів від атакуючого трафіку.

У сучасному Інтернеті DDoS-трафік має багато форм. Трафік може варіюватися від непідроблених атак з одного джерела до складних і адаптивних багатовекторних атак.

Багатовекторна DDoS-атака використовує кілька шляхів атаки, щоб різними способами перевантажити ціль, потенційно відволікаючи зусилля з мінімізації наслідків на будь-якій одній траєкторії.

Прикладом багатовекторної DDoS-атаки є атака, яка націлена на декілька рівнів стека протоколів одночасно, наприклад, посилення DNS (на рівні 3/4) у поєднанні з HTTP-флудом (на рівні 7).

Пом'якшення наслідків багатовекторної DDoS-атаки вимагає різноманітних стратегій для протидії різним траєкторіям.

Загалом, чим складніша атака, тим більша ймовірність того, що атакуючий трафік буде важко відокремити від звичайного трафіку - мета зловмисника полягає в тому, щоб якомога більше злитися з ним, роблячи зусилля з нейтралізації якомога неефективнішими.

Спроби пом'якшення наслідків, які передбачають відключення або обмеження трафіку без розбору, можуть призвести до змішування хорошого трафіку з поганим, а атака також може модифікуватися і адаптуватися, щоб обійти контрзаходи. Для подолання комплексної спроби порушення роботи найбільшу користь принесе багаторівневе рішення.

Маршрутизація чорної діри

Одне з рішень, доступне практично всім мережевим адміністраторам, полягає у створенні маршруту-"чорної діри" і спрямуванні трафіку в цей маршрут. У найпростішій формі, коли фільтрація "чорних дір" реалізована без конкретних критеріїв обмеження, як легітимний, так і зловмисний мережевий трафік спрямовується на нульовий маршрут, або "чорну діру", і виводиться з мережі.

Якщо інтернет-ресурс зазнає DDoS-атаки, провайдер інтернет-послуг (ISP) може перенаправити весь трафік сайту в "чорну діру" в якості захисту. Це не ідеальне рішення, оскільки воно фактично дає зловмиснику бажану мету: робить мережу недоступною.

Обмеження швидкості

Обмеження кількості запитів, які сервер приймає протягом певного проміжку часу, також є способом пом'якшення наслідків атак на відмову в обслуговуванні.

Хоча обмеження швидкості корисне для уповільнення крадіжки контенту веб-скреперами та для запобігання спробам входу методом грубої сили, його самого по собі, швидше за все, буде недостатньо для ефективної протидії складним DDoS-атакам.

Тим не менш, обмеження швидкості є корисним компонентом ефективної стратегії захисту від DDoS-атак.

Брандмауер для веб-додатків

Брандмауер веб-додатків (WAF) - це інструмент, який може допомогти у захисті від DDoS-атак 7-го рівня. Розміщуючи WAF між Інтернетом і вихідним сервером, він може діяти як зворотний проксі-сервер, захищаючи цільовий сервер від певних типів шкідливого трафіку.

Фільтруючи запити на основі низки правил, що використовуються для виявлення інструментів DDoS, можна запобігти атакам 7-го рівня. Однією з ключових переваг ефективного WAF є можливість швидкого впровадження користувацьких правил у відповідь на атаку.

Розсіювання трафіку в мережі Anycast

Цей підхід використовує мережу Anycast для розсіювання трафіку атаки через мережу розподілених серверів до точки, де трафік поглинається мережею.

Подібно до того, як бурхливу річку спрямовують окремими меншими каналами, цей підхід розподіляє вплив розподіленого трафіку атаки до такої міри, що він стає керованим, розсіюючи будь-які зловмисні можливості.

Надійність мережі Anycast для пом'якшення наслідків DDoS-атаки залежить від розміру атаки, а також від розміру та ефективності мережі. Важливою частиною пом'якшення наслідків DDoS-атак, реалізованих Cloudflare, є використання розподіленої мережі Anycast.

Cloudflare має мережу пропускною здатністю 228 Тбіт/с, що на порядок більше, ніж найбільша зафіксована DDoS-атака.

Якщо ви зараз перебуваєте під атакою, є кроки, які ви можете зробити, щоб вийти з-під тиску. Якщо ви вже використовуєте Cloudflare, ви можете виконати ці кроки, щоб пом'якшити наслідки атаки.

Захист від DDoS-атак, який ми впроваджуємо в Cloudflare, є багатогранним, щоб пом'якшити багато можливих векторів атак. Дізнайтеся більше про захист від DDoS у Cloudflare та про те, як він працює [3].

1.3. Мета та завдання захисту корпоративної інформаційної системи від DDoS-атак

Атака на відмову в обслуговуванні (DoS) - це зловмисна спроба вплинути на доступність цільової системи, наприклад, веб-сайту або програми, для законних кінцевих користувачів. Зазвичай зловмисники генерують великі обсяги пакетів або запитів, які зрештою перевантажують цільову систему. У випадку розподіленої атаки на відмову в обслуговуванні (DDoS) зловмисник використовує декілька скомпрометованих або контрольованих джерел для здійснення атаки.

Загалом, DDoS-атаки можна розділити за рівнем моделі взаємодії відкритих систем (OSI), який вони атакують. Найчастіше вони відбуваються на мережевому (3-й рівень), транспортному (4-й рівень), рівні представлення (6-й рівень) та прикладному (7-й рівень) рівнях.

Розглядаючи методи захисту від цих атак, корисно згрупувати їх як атаки на рівні інфраструктури (рівні 3 і 4) і на рівні додатків (рівні 6 і 7).

- Атаки на рівні інфраструктури

Атаки на рівнях 3 і 4 зазвичай класифікуються як атаки на рівні інфраструктури. Вони також є найпоширенішим типом DDoS-атак і включають в себе такі вектори, як синхронізовані (SYN) потоки та інші атаки з відображенням, такі як потоки пакетів користувацьких датаграм (UDP). Ці атаки зазвичай великі за обсягом і мають на меті перевантажити пропускну

здатність мережі або серверів додатків. Але, на щастя, це також тип атак, які мають чіткі сигнатури і їх легше виявити.

- Атаки на рівні додатків

Атаки на рівнях 6 і 7 часто класифікують як атаки на рівні додатків. Хоча ці атаки менш поширені, вони також мають тенденцію бути більш складними. Ці атаки, як правило, невеликі за обсягом порівняно з атаками на рівні інфраструктури, але, як правило, зосереджуються на певних дорогих частинах програми, роблячи її недоступною для реальних користувачів. Наприклад, потік HTTP-запитів на сторінку входу, або дорогий пошуковий API, або навіть XML-RPC-атаки на Wordpress (також відомі як пінгбек-атаки на Wordpress).

Метою захисту корпоративної інформаційної системи від DDoS-атак є забезпечення неперервності роботи бізнес-процесів та збереження цілісності, доступності та конфіденційності інформаційних ресурсів у контексті зростаючих кіберзагроз і складності сучасних інформаційних систем. Основні завдання захисту включають розробку та впровадження ефективних механізмів для виявлення і блокування DDoS-атак, використання передових технологій та інструментів для виявлення ненормального трафіку, підготовку інфраструктури до масштабних та складних атак забезпеченням достатньої пропускної здатності та масштабованості, та розробку планів реагування на інциденти, включаючи процедури відновлення після атак.

Методи захисту від DDoS-атак включають мінімізацію площі атаки, що обмежує можливості зловмисників, дозволяючи концентрувати захисні зусилля в одному місці. Ефективним способом є розміщення обчислювальних ресурсів за мережами розподілу контенту (CDN) або балансувальниками навантаження, а також обмеження прямого інтернет-трафіку до певних частин інфраструктури, таких як сервери баз даних. Використання брандмауерів або списків контролю доступу (ACL) також є ключовим для контролю трафіку, який досягає додатків.

Підготовка до великомасштабних об'ємних DDoS-атак вимагає забезпечення достатньої пропускної здатності та можливості сервера поглинати та пом'якшувати атаки. Важливо, щоб хостинг-провайдер надавав достатню кількість резервних каналів інтернет-з'єднання, щоб обробляти великі обсяги трафіку. Розміщення веб-додатків близько до кінцевих користувачів і на великих інтернет-обмінниках, а також використання мереж розподілу контенту та інтелектуальних служб DNS може забезпечити додатковий рівень мережевої інфраструктури.

Особлива увага має бути приділена обмеженню швидкості, щоб приймати лише стільки трафіку, скільки може обробити хост без шкоди для доступності. Більш просунуті методи захисту включають аналіз окремих пакетів, щоб приймати лише легітимний трафік, розуміючи характеристики нормального трафіку.

Використання брандмауера веб-додатків (WAF) є ключовим для захисту від складних атак, таких як SQL-ін'єкції або підробка міжсайтових запитів. Це дозволяє створювати індивідуальні засоби захисту від незаконних запитів, які можуть маскуватися під нормальний трафік або надходити з підозрілих джерел. Іноді досвідчена підтримка може бути корисною для вивчення шаблонів трафіку та розробки індивідуальних засобів захисту [4].

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ ВІД DDOS-АТАК

2.1. Аналіз існуючих технологій захисту інформаційної системи організації від DDoS-атак

Одним із найпотужніших засобів захисту від розподілених атак типу "відмова в обслуговуванні" (DDoS) є доступ до послуг захисту від DDoS. Ці рішення діють як щит, гарантуючи, що веб-сайти організації залишаються захищеними від руйнівних атак. Наведені нижче постачальники - це вибірка найкращих постачальників послуг захисту від DDoS-атак на сучасному ринку, більшість з яких можна використовувати в будь-якій галузі, від ігор та електронної комерції до виробництва та енергетики.

1. Cloudflare: Найкращий постачальник послуг із захисту від DDoS;
2. Radware: найкращий постачальник індивідуальних, масштабованих рішень для захисту від DDoS-атак;
3. Imperva: Найкращий для миттєвого захисту від DDoS з високою потужністю;
4. Amazon Web Services: Найкращий за масштабований захист в інфраструктурі AWS;
5. GCore: Найкращий для захисту від ботів у реальному часі, периферійної інфраструктури;
6. Akamai: Найкращий для захисту від загроз додатків;
7. Ribbon: Найкращий для розширеного виявлення DDoS-атак і боротьби з ними;
8. Vercara: Найкраще рішення для широкомасштабного захисту в різних інфраструктурах;
9. NetScout: Найкраще для гібридних, адаптивних рішень для захисту від DDoS.

Більшість з перелічених постачальників отримали високі бали в рейтингу Forrester DDoS Wave. Окрім захисту від традиційних DDoS-атак, вони використовують хмарні, мобільні та IoT-функції, а також ключові функції та сервіси.

Cloudflare

Хмарна система захисту від DDoS, пропонована Cloudflare, забезпечує оборону проти атак 7-го рівня, а також 3-го та 4-го рівнів, використовуючи глобальну мережу, замість спеціалізованого обладнання. Це рішення захищає веб-сайти, додатки та цілі мережі без порушення продуктивності легітимного трафіку.

Особливості Cloudflare включають мережу з пропускною здатністю 100 Тбіт/с, здатну блокувати в середньому 76 мільярдів загроз на день. Ця система підтримує безперервний захист від DDoS-атак на веб-ресурси з використанням аналітики, отриманої з глобальної мережі Cloudflare, та працює в тандемі з хмарним брандмауером веб-додатків (WAF) для захисту від кібер- та мережевих загроз.

Cloudflare Spectrum забезпечує захист від DDoS-атак для будь-яких додатків, що працюють по протоколу TCP/UDP, з вбудованим балансуванням навантаження і прискоренням трафіку, а Cloudflare Magic Transit захищає мережеву інфраструктуру від DDoS-атак на основі протоколу BGP.

Центри обробки даних анонсують клієнтські підмережі, щоб зменшувати загрози поблизу джерела атаки. Система використовує як централізовані, так і децентралізовані механізми захисту для швидкого виявлення та усунення DDoS-атак, а також вбудовану аналітику для моніторингу шаблонів трафіку.

Переваги Cloudflare включають широку глобальну мережу, розширені функції захисту, безшовну інтеграцію з різними сервісами та інтуїтивно зрозумілу інформаційну панель. Сервіс також пропонує безкоштовний рівень захисту. Однак система має деякі недоліки, такі як сильна залежність від

інфраструктури Cloudflare, складності з ціноутворенням індивідуальних планів та обмежена підтримка для нижчих тарифних планів.

Radware

Radware надає рішення для захисту від DDoS-атак, яке підходить для різноманітних інфраструктур, включаючи публічні хмари, підприємства та постачальників послуг. Це рішення включає захист центрів обробки даних, приватних і публічних хмар, а також інфраструктури 5G, і є агностичним до середовища, спеціально розробленим для допомоги провайдерам послуг у захисті великомасштабних мереж.

Рішення Radware характеризується такими особливостями:

- Автоматизований захист від DDoS-атак нульового дня для широкого покриття безпеки.
- Гібридні варіанти розгортання хмарного DDoS-сервісу з постійним і на вимогу підключенням.
- Хмарний захист на рівні SSL, що забезпечує конфіденційність даних.
- Єдина скляна панель з уніфікованим порталом і керованим сервісом від команди реагування на надзвичайні ситуації.
- Інтегрований захист веб-додатків для захисту додатків і мережі.
- Поєднання постійного виявлення і пом'якшення наслідків з хмарним об'ємним запобіганням DDoS-атакам.

Переваги цього рішення включають індивідуальний підхід до різних інфраструктур, забезпечення широкого і ефективного фокусу на запобіганні та пом'якшенні наслідків атак, а також надання єдиного порталу для моніторингу. Рішення може адаптуватися до потреб різних клієнтів, включаючи телекомунікаційні та хмарні оператори.

Недоліки рішення Radware можуть включати відносно складну конфігурацію та налаштування, високу вартість порівняно з деякими конкурентами, а також можливі проблеми з інтеграцією з існуючими системами.

Imperva

Система захисту від DDoS-атак, розроблена Imperva, спроможна ефективно впоратися з будь-яким типом ресурсів, забезпечуючи швидке усунення наслідків атаки протягом трьох секунд. Простота впровадження та експлуатації системи досягається завдяки використанню готових політик та самоадаптивних налаштувань.

Imperva Attack Analytics надає чітке уявлення про різні типи та рівні атак, прискорюючи процес розслідування та зменшуючи втому від постійної готовності до реагування. Imperva ефективно працює в різних секторах, включаючи електронну комерцію, енергетику, фінансові послуги, ігрову індустрію, охорону здоров'я, виробництво та технології.

Можливості системи включають захист веб-сайтів, мереж, DNS та окремих IP-адрес. Система ефективно зупиняє атаки рівнів 3, 4 і 7, маючи пропускну здатність 9 Тбіт/с та 65 GPP. Її однорівнева архітектура стеку забезпечує мінімальну затримку та швидке усунення атак. У кожній з 50 точок присутності (PoP) глобальної мережі Imperva надаються всі послуги безпеки. Система забезпечує реальночасову видимість DDoS-загроз з детальним звітуванням та можливістю інтеграції з SIEM.

Переваги Imperva включають трисекундну угоду про рівень обслуговування (SLA) для будь-якої DDoS-атаки, реальночасову аналітику атак та самоадаптивні політики безпеки. Однак система має деякі недоліки, такі як відсутність прозорої інформації про ціни, обмежені можливості кастомізації та необхідність суворого дотримання SLA для забезпечення оптимальної продуктивності.

Amazon Web Services

AWS Shield є керованою службою захисту від DDoS-атак, яка надає захист для програм, що працюють на Amazon Web Services. Вона спеціалізується на захисті від поширених мережевих та транспортних рівнів атак, часто спрямованих на веб-сайти та додатки. AWS Shield забезпечує

постійне виявлення та автоматичне усунення наслідків атак, мінімізуючи час простою та затримки.

Клієнти AWS автоматично користуються перевагами AWS Shield Standard без додаткових витрат, що забезпечує захист від більшості поширених DDoS-атак. Це рішення може використовуватися разом з Amazon CloudFront та Amazon Route 53 для комплексного захисту.

AWS Shield Advanced пропонує додаткове виявлення та пом'якшення складних DDoS-атак, відстеження атак майже в реальному часі та інтеграцію з AWS WAF, а також надає доступ до команди реагування AWS Shield Response Team (SRT) та захист для Amazon EC2, ELB, Amazon CloudFront, AWS Global Accelerator та Amazon Route 53.

Переваги AWS Shield включають масштабований захист для всієї AWS інфраструктури, наявність різних рівнів захисту, просту інтеграцію з AWS сервісами та безкоштовний стандартний рівень захисту. Також відзначається легкість налаштування та конфігурації.

Однак, є й недоліки, такі як потенційно висока вартість залежно від використання та рівня, залежність від інфраструктури та сервісів AWS, а також можливі обмеження у порівнянні зі спеціалізованими рішеннями.

GCore

GCore пропонує послуги захисту від DDoS-атак, орієнтовані на веб-додатки та сервери, за допомогою периферійної хмарної інфраструктури. Ці послуги забезпечують захист на мережевому (L3) та транспортному (L4) рівнях, а також включають захист від ботів у реальному часі та брандмауер нового покоління (NGFW). GCore також пропонує можливість розробки кастомних функцій для задоволення специфічних потреб бізнесу.

Серед основних функцій GCore - захист від ботів у реальному часі, який блокує небажаний трафік ботів, націлений на веб-сайти та API. Компанія має понад 140 точок присутності (PoP) на п'яти континентах, підтримує HTTP/2, IPv6, веб-сокети та зосереджена на блокуванні сесій, а не окремих IP-адрес. GCore також пропонує варіанти балансування

навантаження, включаючи циклічний, зважений циклічний та IP-хешування, і може бути упакований з іншими пропозиціями компанії, як-от універсальна платформа для потокового мовлення та глобальний хостинг.

Перевагами GCore є захист від ботів у реальному часі та NGFW, фокус на периферійній хмарній інфраструктурі, можливість комбінування з іншими послугами GCore, високі можливості обробки та фільтрації трафіку, а також безкоштовні рівні для новачків. Однак, компанія може мати складні моделі ціноутворення з багаторівневими пропозиціями та мінімальним рівнем зобов'язань, а також можливі обмеження в налаштуванні під конкретні потреби [5].

2.2. Призначення, можливості та функції Cloudflare

Cloudflare є сервісом мережі доставки контенту (CDN) та хмарною платформою для захисту, який пропонує послуги забезпечення безпеки, оптимізації та підвищення продуктивності веб-сайтів, підключених до нього.

До основних функцій Cloudflare входять:

- налаштування кешування та оптимізації для покращення швидкості завантаження,
- захист від цифрових загроз, включно з DDoS-атаками,
- управління DNS-записами,
- перехід веб-сайту на захищене HTTPS-з'єднання,
- аналіз веб-трафіку.

Cloudflare автоматично виявляє та пом'якшує атаки розподіленої відмови в обслуговуванні (DDoS)через автономні системи DDoS.

Ці системи включають численні динамічні правила пом'якшення, які представлені як керовані набори правил захисту від атак DdoS [6].

Захист від DDoS

Для виявлення та пом'якшення наслідків DDoS-атак автономні периферійні та централізовані DDoS-системи Cloudflare аналізують зразки трафіку поза маршрутом, що дозволяє Cloudflare асинхронно виявляти DDoS-атаки, не викликаючи затримок та не впливаючи на продуктивність.

Аналізовані зразки включають в себе:

- Поля пакетів, такі як IP-адреса джерела, порт джерела, IP-адреса призначення, порт призначення, протокол, прапори TCP, порядковий номер, опції та швидкість передачі пакетів.
- Метадані HTTP-запиту, такі як заголовки HTTP, агент користувача, рядок запиту, шлях, хост, метод HTTP, версія HTTP, версія шифру TLS і швидкість запиту.
- Метрики HTTP-відповіді, такі як коди помилок, повернуті серверами походження клієнтів, і їхні швидкості.

Як тільки атакуючий трафік відповідає правилу, системи Cloudflare відстежують цей трафік і генерують сигнатуру в реальному часі, щоб зіставити його з шаблоном атаки і пом'якшити атаку, не впливаючи на легальний трафік. Правила здатні генерувати різні сигнатури на основі різних властивостей атак і рівня сигналу кожного атрибуту. Наприклад, якщо атака є розподіленою, тобто походить з багатьох вихідних IP-адрес, то поле вихідної IP-адреси не буде служити сильним індикатором, і правило не буде вибирати поле вихідної IP-адреси як частину сигнатури атаки. Після створення відбиток поширюється як правило усунення атаки в найбільш оптимальне місце в глобальній мережі Cloudflare для економічно ефективного усунення атаки. Ці правила усунення наслідків є ефемерними і втрачають чинність незабаром після завершення атаки, що відбувається, коли ніякий додатковий трафік не відповідає цьому правилу [7].

2.3. Особливості використання Cloudflare для захисту інформаційних систем від DDoS-атак

1. Керовані набори правил

Керовані набори правил захисту від атак DDoS забезпечують комплексний захист від різноманітних атак DDoS на рівнях L3/4 (мережевий рівень) і L7 (рівень прикладних програм) моделі OSI..

Доступні керовані набори правил:

- Захист від HTTP DDoS атак

Цей набір правил містить правила для виявлення та пом’якшення атак DDoS через HTTP і HTTPS.

- Захист від атак DDoS на мережевому рівні

Цей набір правил містить правила для виявлення та пом’якшення атак DDoS на L3/4 моделі OSI, таких як затоплення UDP, атаки відбиття SYN-ACK, затоплення SYN і затоплення DNS.

Проактивне помилкове виявлення нових правил

Коли Cloudflare створює нове кероване правило, перевіряється його вплив на трафік зон Business і Enterprise, поки правило ще не блокує трафік.

У разі виявлення хибного спрацьовування Cloudflare завчасно зв’язується з постраждалими клієнтами та допомагають їм внести зміни в конфігурацію (наприклад, знизити рівень чутливості нового правила), перш ніж правило почне зменшувати трафік. Це запобігає тому, що нове правило спричиняє збої в роботі послуг і збої в роботі Інтернет-ресурсів [8].

2. Адаптивний захист від DdoS

Адаптивний захист від DDoS-атак вивчає унікальні шаблони трафіку користувача та адаптується до них, щоб забезпечити кращий захист від складних атак DDoS на рівні 7 і рівнях 3/4, залежно від служб Cloudflare.

Адаптивний захист від DDoS забезпечує наступні типи захисту:

- Захист для джерел: виявляє та пом’якшує трафік, який відхиляється від профілю помилок джерела сайту користувача.

- Захист для користувацьких агентів: виявляє та пом’якшує трафік, який відхиляється від найкращих користувацьких агентів, які Cloudflare бачить у мережі. Профіль User Agent будується з усієї мережі Cloudflare, а не тільки з зони клієнта.
- Захист для розташування: виявляє та пом’якшує трафік, який відхиляється від профілю георозповсюдження сайту організації. Профіль розраховується на основі курсу для кожної клієнтської країни та регіону, використовуючи курси за останні сім днів.
- Захист для протоколів: виявляє та пом’якшує трафік, який відхиляється від профілю IP-протоколу трафіку організації.

Адаптивний захист від DDoS-атак створює профіль трафіку, переглядаючи максимальні показники трафіку щодня за останні сім днів. Ці профілі перераховуються щодня, зберігаючи семиденне часове вікно. Адаптивний захист від DDoS-атак зберігає максимальні показники трафіку для кожного попередньо визначеного значення параметра (розмір профілювання змінюється для кожного правила). Кожен профіль використовує один вимір, як-от країна джерела запиту, агент користувача та IP-протокол. Вхідний трафік, який відхиляється від профілю користувача, може бути шкідливим.

Щоб усунути викиди, підрахунок ставки враховує лише 95-й процентиль ставок (відкидаючи верхні 5% найвищих ставок). Крім того, правила адаптивного захисту від DDoS-атак також враховують моделі машинного навчання Cloudflare (ML), щоб ідентифікувати трафік, який, імовірно, автоматизований.

Cloudflare може час від часу змінювати логіку цих правил захисту, щоб покращити їх. Будь-які зміни правил відображатимуться на сторінці журналу змін керованих наборів правил .

3. Захист від DDoS на основі частоти помилок HTTP джерела

Мережа Cloudflare створена для автоматичного моніторингу та пом’якшення великих DDoS-атак. Cloudflare також допомагає пом’якшити невеликі DDoS-атаки на основі таких загальних правил:

- Для зон у будь-якому плані Cloudflare застосовуватиме пом’якшення, коли частота помилок HTTP перевищує високий (за замовчуванням) рівень чутливості 1000 помилок на секунду. Користувач може зменшити рівень чутливості, налаштувавши керований набір правил захисту від атак HTTP DDoS .
- Для зон у планах Pro, Business і Enterprise Cloudflare виконує додаткову перевірку для кращої точності виявлення: частота помилок за секунду також має принаймні в п’ять разів перевищувати звичайний рівень вихідного трафіку перед застосуванням засобів пом’якшення DDoS.

Cloudflare визначає частоту помилок на основі всіх помилок HTTP в діапазоні 52X (внутрішня помилка сервера) і в діапазоні 53X, за винятком помилки 530 . Наразі для пом’якшення DDoS на основі частоти помилок HTTP не можна виключити певні коди помилок HTTP.

Для аналізу трафіку, ідентифікованого за допомогою HTTP Adaptive DDoS Protection в сервісі Cloudflare, необхідно виконати ряд дій на інформаційній панелі сервісу. Спочатку слід авторизуватися в системі Cloudflare, обравши відповідний обліковий запис та веб-сайт. Далі потрібно перейти до розділу "Безпека" та підрозділу "Події", де за допомогою фільтру за сервісом "HTTP DDoS" та ідентифікатором правила можна переглянути відповідний трафік.

Для правил адаптивного захисту від DDoS атак 3-го та 4-го рівнів наразі рекомендується використовувати інструменти Logpush або GraphQL API для перегляду позначеного трафіку.

Налаштування дій та чутливості правил Адаптивного захисту від DDoS є важливим кроком у конфігурації захисту. Зазвичай використовується дія "журнал" для моніторингу позначеного трафіку перед прийняттям рішення про дію пом'якшення. Детальні інструкції з налаштування захисту від HTTP

DDoS-атак на інформаційній панелі для правил 7-го рівня, а також налаштування захисту мережевого рівня від DDoS-атак для правил 3-го і 4-го рівнів, можна знайти в відповідних розділах інформаційної панелі Cloudflare [9].

4. Розширений захист TCP

Cloudflare Advanced TCP Protection, базована на механізмі flowtrackd, є інструментом перевірки TCP із збереженням стану. Вона використовується для виявлення та пом’якшення складних атак TCP поза межами стану, включаючи рандомізовані та підроблені затоплення ACK або затоплення SYN і SYN-ACK. Advanced TCP Protection здатна захищати від різноманітних видів атак, включаючи точні атаки, націлені на певну комбінацію IP/порт призначення, та широкомасштабні атаки, націлені одночасно на кілька IP-адрес одного IP префікса. Також вона забезпечує моніторинг TCP-з’єднань, навіть при їх переміщенні між центрами обробки даних Cloudflare.

Advanced TCP Protection доступна для всіх клієнтів Magic Transit і є вимкненою за замовчуванням, але включає захист від простіших DDoS-атак на основі TCP як частину керованого набору правил захисту від DDoS-атак мережевого рівня. Щоб розпочати роботу з Advanced TCP Protection, необхідно перейти до налаштувань у відповідному розділі.

Advanced TCP Protection пропонує два типи захисту: захист від затоплення SYN, що захищає від атак, таких як повністю рандомізовані затоплення SYN і SYN-ACK, та захист TCP поза межами штату, який захищає від атак TCP DDoS поза межами стану, таких як повністю рандомізовані ACK-затоплення та RST-затоплення. Кожен тип захисту налаштовується незалежно через правила і, за потреби, фільтри. Існують конкретні параметри конфігурації для правил затоплення SYN та TCP за межами штату, які можна знайти у відповідних розділах інструкцій [10].

5. Розширений захист DNS (бета)

Cloudflare Advanced DNS Protection Beta, розроблена на основі flowtrackd, надає захист із збереженням стану від складних DDoS-атак на

основі DNS, у тому числі тих, що використовують рандомізовані префікси DNS. Система вивчає шаблони трафіку користувача, формуючи базову лінію типу DNS-запитів, яка дозволяє відрізняти легітимні запити від зловмисних, надаючи захист без негативного впливу на законний трафік. Наразі система обмежена аналізом лише DNS через UDP.

Інформаційна панель мережевої аналітики відображає системну аналітику для розширеного захисту DNS, включаючи запитувані домени та типи записів. Розширений захист DNS доступний у бета-версії для клієнтів Magic Transit, а захист від простіших DDoS-атак на основі DNS включено як частина керованого набору правил захисту від DDoS-атак мережевого рівня.

Наразі конфігурація розширеного захисту DNS не доступна через інформаційну панель Cloudflare або Cloudflare API, і клієнти повинні звернутися до команди свого облікового запису для увімкнення цієї функції та виконання початкової конфігурації. Вбудовані префікси надаються разом з Advanced TCP Protection, і якщо клієнт уже налаштував необхідні префікси для розширеного захисту TCP, додаткові дії для Advanced DNS Protection не потрібні.

У разі проблем зі збором даних пов’язаних із Advanced DNS Protection, можливі причини включають відсутність доданих префіксів до розширеного захисту TCP, неактивність системи Advanced DNS Protection або відсутність DNS-трафіку через UDP.

Cloudflare також збирає DNS-дані, такі як тип запиту та запитувані домени. Щоб вимкнути цей збір даних, клієнти повинні видалити свої префікси з інформаційної панелі Cloudflare або за допомогою API. Це також видалить префікси з Advanced DNS Protection і Advanced TCP Protection.

Як доповнення до розширеного захисту DNS, для кешування DNS, проксі-сервера та конфігурації може використовуватися брандмауер DNS Cloudflare. Наразі розширений захист DNS не доступний для брандмауера DNS [11].

3 РОЗРОБЛЕННЯ ВАРІАНТУ ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ ВІД DDOS-АТАК НА БАЗІ CLOUDFLARE

3.1. Варіант розгортання Cloudflare для захисту інформаційної системи організації

Cloudflare представляє собою глобальну мережу серверів, що забезпечує користувачам можливість підключення веб-сайтів для підвищення швидкості завантаження та забезпечення захисту від DDoS-атак. Додатково, ця платформа надає функціонал для управління DNS-записами в домені користувача та переходу веб-сайтів на безпечне HTTPS-з'єднання.

В рамках послуг Cloudflare, пропонуються як безкоштовні, так і платні тарифні плани. Вибір конкретного тарифу впливає на рівень наданого захисту та можливості оптимізації роботи сайту.

У контексті забезпечення ефективності веб-сайтів, Cloudflare використовує технологію CDN (Content Delivery Network - мережу доставки контенту) для оптимізації часу завантаження сторінок. Ця технологія полягає у розподіленні кешованих статичних файлів веб-сайту, включаючи зображення, CSS та JavaScript, на мережу серверів Cloudflare, розміщених по всьому світу. Коли користувач намагається перейти до веб-сайту, ці файли надсилаються з найближчого сервера до географічного розташування користувача. Така модель дистрибуції знижує загальне навантаження на первинний хостинг сайту та скорочує латентність передачі даних, оскільки вони подолають значно коротшу дистанцію до кінцевого користувача.

Методика захисту від DDoS-атак, імплементована компанією Cloudflare, базується на ретельному моніторингу та фільтрації вхідного трафіку до веб-сайтів. В рамках цієї системи, всі запити, які надходять до веб-сайту, спочатку проходять через інфраструктуру Cloudflare. Функціонуючи як передова лінія оборони, Cloudflare аналізує трафік,

виявляючи і блокуючи запити, які містять ознаки шкідливості або підозрілості. Запити, які класифікуються як безпечні, пересилаються далі до цільового сайту. Цей механізм дозволяє ефективно протистояти різним формам DDoS-атак, тим самим знижуючи ймовірність зайвого навантаження на ресурси веб-сайту внаслідок масового несанкціонованого трафіку.

Інтеграція Cloudflare з веб-сайтом починається з реєстрації на офіційному сайті Cloudflare, де користувач має натиснути на кнопку «Sign up», розташовану в правому верхньому куті головної сторінки. Далі, в процесі створення облікового запису, користувачу потрібно вказати адресу електронної пошти як ім'я користувача та створити пароль, який має містити мінімум 8 символів, у тому числі цифру та спеціальний символ, і підтвердити створення акаунту.

Після реєстрації, користувач вводить домен для його зв'язку з Cloudflare, вибирає тарифний план, наприклад, безкоштовний, та продовжує процес. Cloudflare проводить сканування DNS-зони домену, автоматично знаходить існуючі DNS-записи та створює їх у своїй системі. Якщо потрібно, користувач може додати відсутні записи вручну.

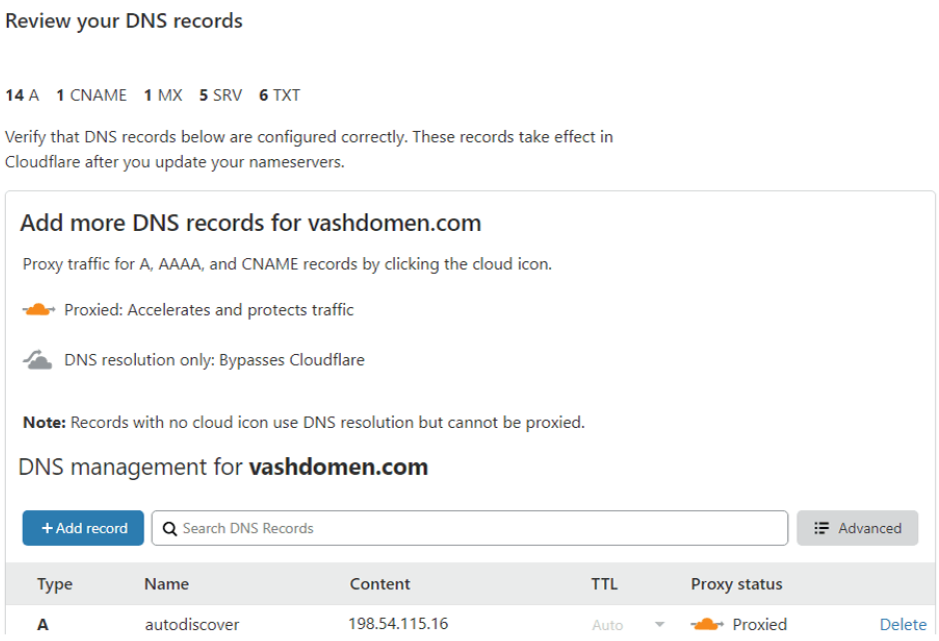

Рис.3.1. Процес сканування DNS-зони домену користувача

Налаштування DNS-серверів: На наступній сторінці вказуються DNS-сервери Cloudflare, які необхідно встановити в налаштуваннях домену на сайті реєстратора домену

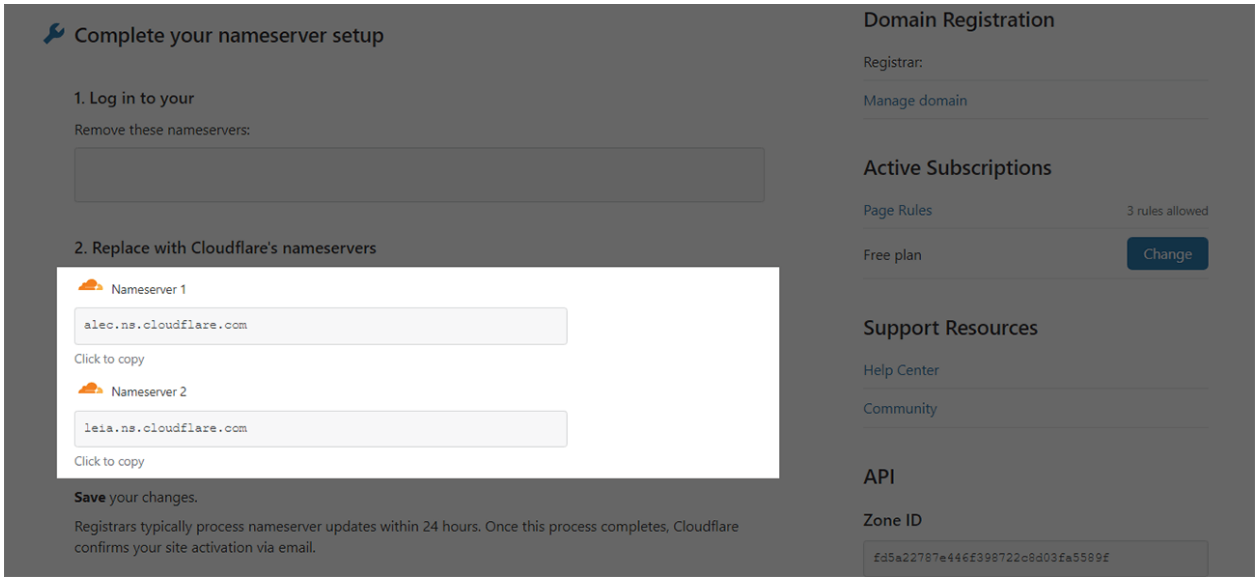

Рис.3.2. Сторінка налаштування DNS-серверів Cloudflare

Управління функціями Cloudflare: Після спрямування домену на Cloudflare, користувач отримує доступ до різних функцій, включаючи кешування, управління DNS, SSL/TLS, Firewall і Page Rules

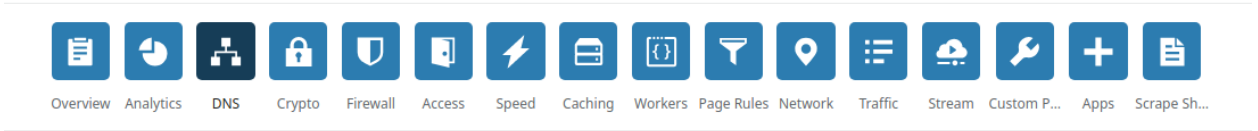

Рис.3.3. Панель управління Cloudflare

- Керування кешем:

Налаштування кешування здійснюється через вкладку "Caching", де можна очистити кеш повністю або частково

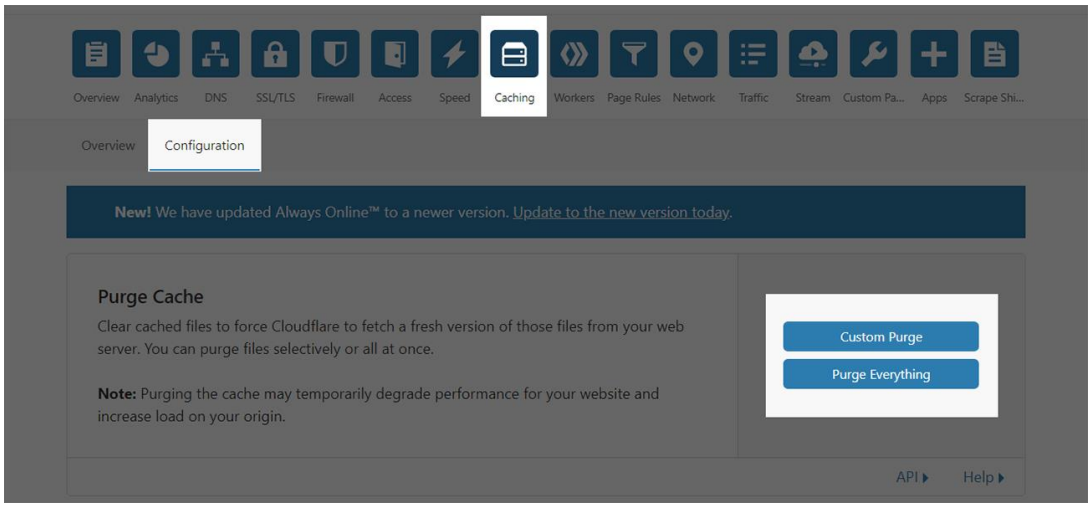

Рис. 3.4. Налаштування кешування

- Робота з DNS-записами:

У розділі "DNS" можна управляти DNS-записами, вносячи зміни або додаючи нові записи

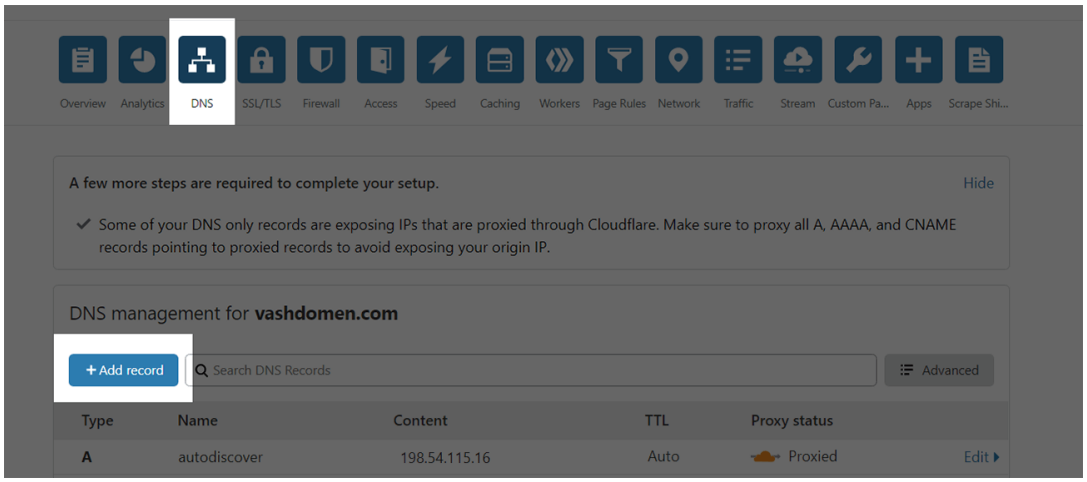

Рис.3.5. Управління DNS-записами

Розглянемо процедуру створення A-запису для субдомену, використовуючи як приклад субдомен "blog". Спочатку необхідно вибрати тип DNS-запису "A" у відповідному інтерфейсі управління DNS. Далі слід заповнити обов'язкові поля для цього запису:

- Поле "Name": Вказується ім'я хоста в межах домену, для якого створюється запис. У випадку створення запису для основного домену,

вводиться символ "@". Для субдомену, наприклад "blog.vashdomen.com", необхідно вказати лише назву субдомену "blog", відокремлену від основного домену.

- Поле "IPv4 address": В це поле вноситься IP-адреса, яка буде асоційована з вказаним хостом. Залежно від типу DNS-запису, це поле може мати різні назви та значення, але його основна функція полягає у визначенні цільового ресурсу, який може бути представлений текстом, доменом або URL.
- Поле "TTL" (Time To Live): Це значення визначає час життя DNS-запису в кеші DNS-сервера користувача. Вище значення TTL збільшує час, протягом якого інформація про запис зберігатиметься, перш ніж буде запитана оновлена інформація. У випадку активації проксі-функції Cloudflare, параметр TTL автоматично налаштовується на "Auto".
- Поле "Proxy status": Це поле визначає, чи буде DNS-запис оброблятися через проксі-сервери Cloudflare. При встановленні статусу "Proxied", всі запити до цього DNS-запису проходитимуть через Cloudflare, що активує всі функції сервісу, включаючи CDN, SSL та захист від DDoS-атак. У разі вибору "DNS Only", запити будуть проходити безпосередньо, без використання додаткових функцій Cloudflare.

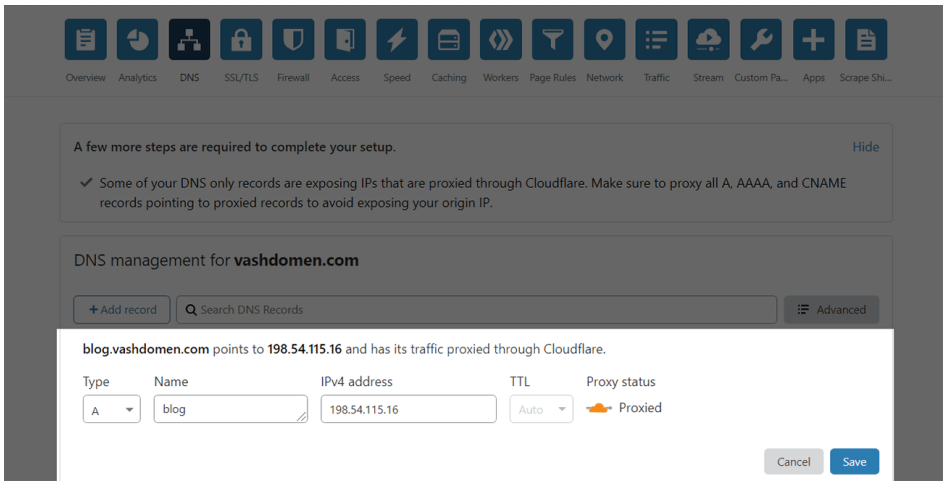

Рис. 3.6. Створення A-запису для субдомену

- Налаштування HTTPS:

В розділі "SSL/TLS" користувачі можуть налаштувати параметри SSL, включаючи режими "Full" та "Flexible"

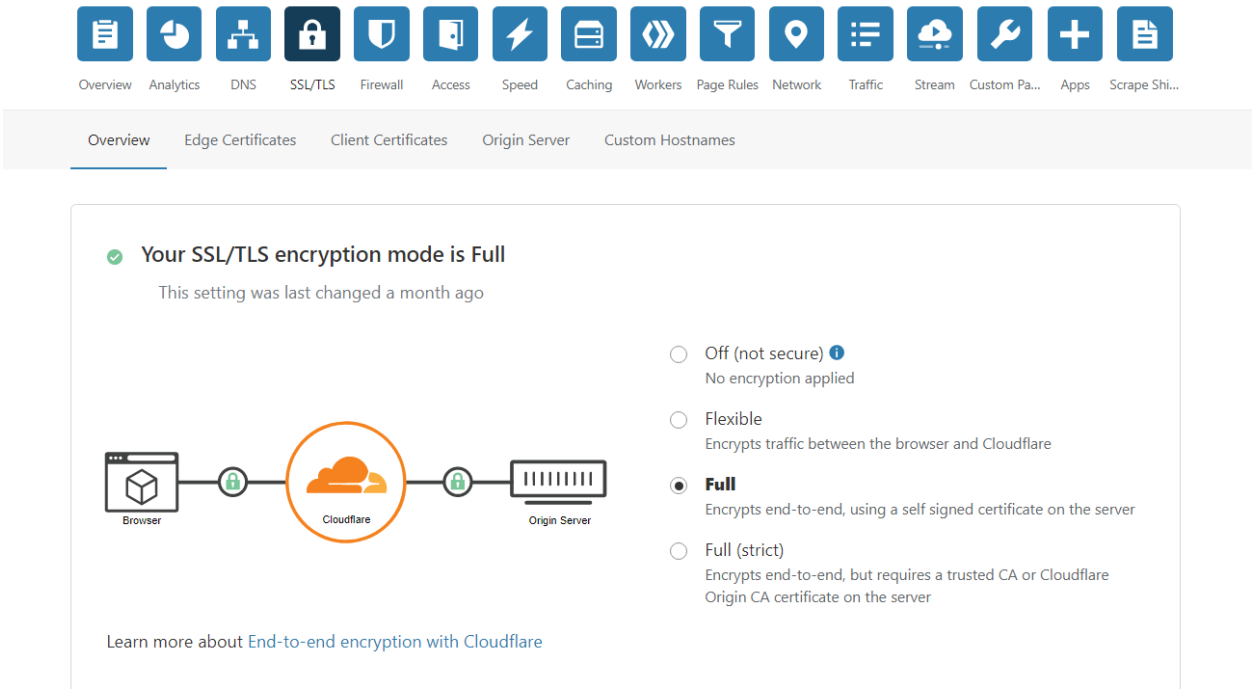

Рис.3.7. Налаштування SSL/TLS

Забезпечення безпеки з'єднань у веб-просторі є критично важливим, особливо в контексті захисту даних користувачів. Cloudflare використовує свій власний безкоштовний SSL-сертифікат під назвою Universal SSL для захисту з'єднань від користувача до Cloudflare. Цей сертифікат автоматично активується після додавання домену до облікового запису Cloudflare, забезпечуючи шифрування на першому сегменті шляху з'єднання.

Далі необхідно взяти до уваги з'єднання між Cloudflare та кінцевим сервером веб-сайту. Якщо на сервері веб-сайту вже встановлено SSL-сертифікат, рекомендується вибрати режим "Full (Strict)" у налаштуваннях Cloudflare. Це забезпечить повне шифрування всього шляху з'єднання від користувача до сервера веб-сайту.

У випадку відсутності SSL-сертифіката на хостингу сервера, можливо вибрати режим "Flexible" в Cloudflare. Однак, це створює певний ризик безпеки, оскільки з'єднання між Cloudflare та сервером веб-сайту буде відбуватися без шифрування, що теоретично дозволяє третім особам перехоплювати дані. Такий режим слід розглядати лише як тимчасовий захід або у випадках, коли встановлення SSL-сертифіката на сервері не є можливим.

Наявність режиму "Full" або "Full (Strict)" без відповідного SSL-сертифіката на сервері може призвести до помилок підключення для користувачів, зокрема до відображення помилок 525 або 526, що індикують проблеми зі SSL-з'єднанням. Ці помилки, хоча й схожі візуально, мають різницю у кодах, що вказують на конкретну проблему в SSL-підключенні.

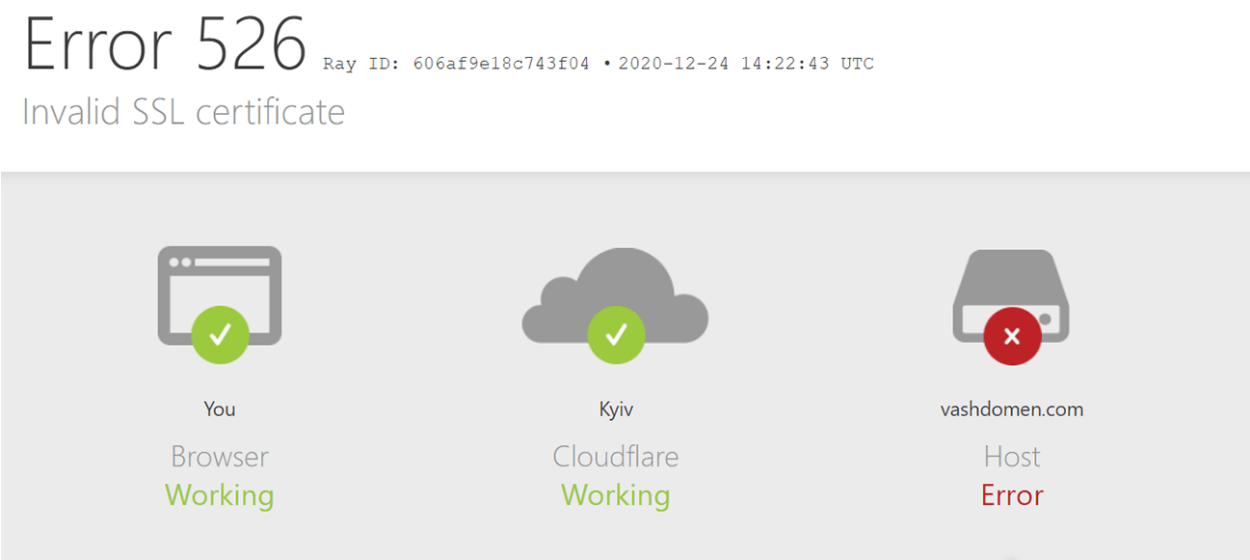

Рис.3.8. Відображення помилки 526, яка індикує проблеми зі SSL-з'єднанням

Після вибору відповідного режиму безпеки, рекомендується провести перевірку шляхом введення домену сайту в браузері з використанням HTTP. У випадку, якщо сайт автоматично перенаправляє на HTTPS-версію, це свідчить про коректну роботу SSL-забезпечення. У разі, якщо сайт відкривається у версії HTTP, це означає, що сайт доступний і через незахищене з'єднання. Для вирішення цієї проблеми можна активувати опцію

"Always Use HTTPS" у налаштуваннях SSL/TLS у розділі "Edge Certificates" Cloudflare. Це забезпечить автоматичне перенаправлення всіх запитів на захищену HTTPS-версію сайту, підвищуючи рівень безпеки з'єднання.

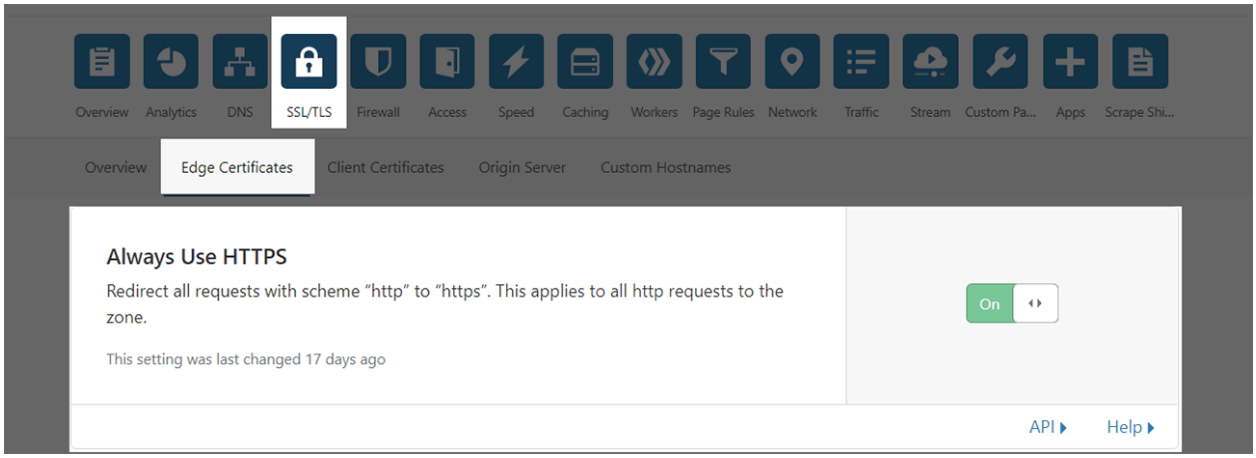

Рис.3.9. Активація опції "Always Use HTTPS"

- Захист від DDoS-атак:

Включення режиму "I'm Under Attack!" у розділі "Firewall" для підвищення захисту сайту від DDoS-атак.

Підключення веб-сайту до Cloudflare вже саме по собі забезпечує базовий рівень захисту від DDoS-атак. Специфіка Cloudflare полягає у приховуванні реальної IP-адреси сервера, на якому розміщений веб-сайт, перенаправляючи потенційні атаки на свої власні сервери. Це дозволяє Cloudflare фільтрувати підозрілий трафік, блокуючи потенційно шкідливі запити, в той час як легітимний трафік продовжує надходити на сайт.

Кешування, що реалізовано Cloudflare, також має значення у захисті від DDoS-атак, оскільки знижує навантаження на оригінальний хостинг сайту. Однак, при наявності активної DDoS-атаки, рекомендується додатково налаштовувати параметри безпеки в обліковому записі Cloudflare. Незважаючи на те, що безкоштовний тариф надає захист від найпоширеніших типів DDoS-атак (зокрема, 3, 4 та 7 рівнів атак), комплексний захист вимагає використання платних тарифів.

Однією з ключових функцій Cloudflare є режим "I’m Under Attack!", який активує додаткові заходи перевірки відвідувачів сайту.

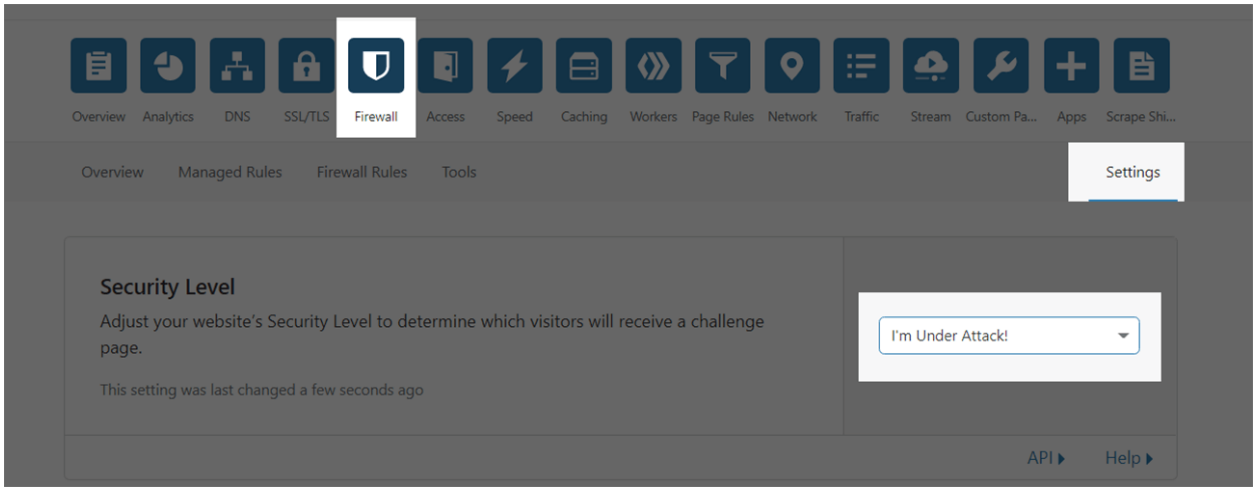

Рис. 3.10. Ввімкнення режиму "I’m Under Attack!"

В цьому режимі всі користувачі спочатку бачать повідомлення, яке дозволяє Cloudflare відрізнити легітимний трафік від шкідливого. Для активації цього режиму, необхідно перейти до розділу "Firewall" в обліковому записі Cloudflare, вибрати вкладку "Settings" і змінити рівень безпеки на "I’m Under Attack!" у блоку "Security Level". За замовчуванням, перевірений відвідувач отримує доступ до сайту на обмежений час, який може бути налаштований у вкладці "Challenge Passage". По завершенні атаки режим "I’m Under Attack!" слід вимкнути, щоб не створювати зайвих перешкод для користувачів сайту.

У випадках, коли потрібен привентивний захист, але без суттєвого обмеження доступу для користувачів, варто вибрати режим безпеки "High". У цьому випадку Cloudflare також використовує перевірку користувачів, але фокусується на тих, чиї IP-адреси були раніше зазначені як підозрілі протягом останніх 14 днів.

- Налаштування правил доступу

Ці правила дозволяють обмежити доступ до вебсайту, змушуючи відвідувачів проходити через CAPTCHA або виконувати блокування на основі географічного розташування, типу запиту, IP-адреси, діапазону IP-

адрес, або User Agent. В межах безкоштовного плану Cloudflare можна створити до п'яти правил доступу. Для цього необхідно перейти до розділу «Firewall», вибрати вкладку «Firewall Rules» та використати функцію «Create a Firewall rule».

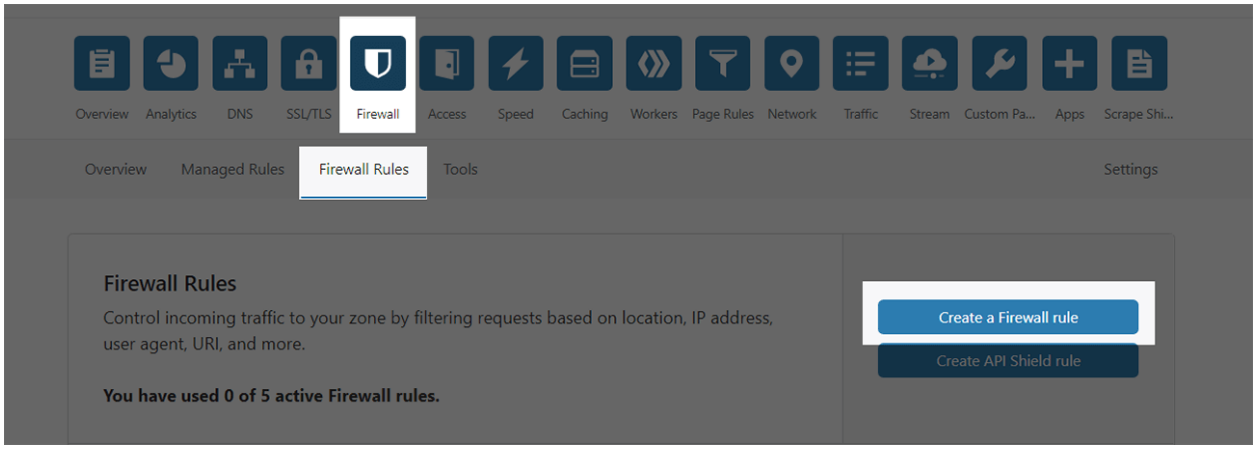

Рис.3.11. Створення правила доступу

Наприклад, для блокування трафіку з певних IP-адрес або діапазону адрес, можна створити правило з відповідною назвою, наприклад, «Блокування трафіку».

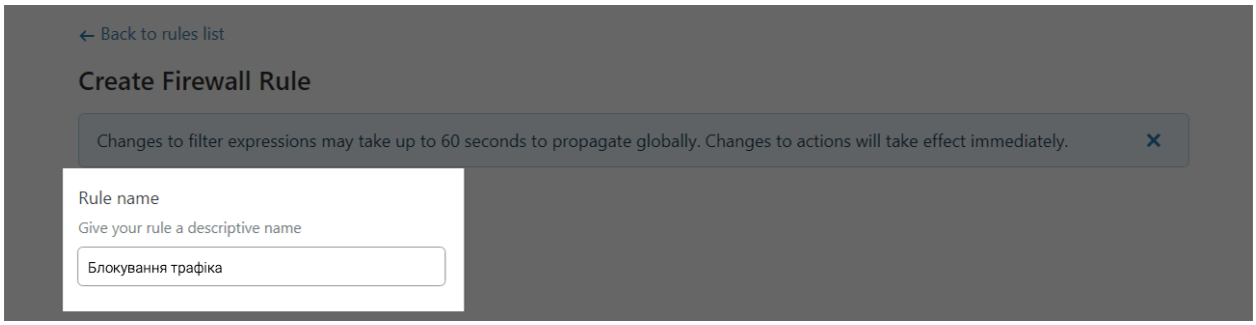

Рис.3.12 Створення правила для блокування трафіку

Поля деталей правила включають:

- Field — параметр, що використовується для фільтрації трафіку. Наприклад, може бути вибрано «IP address».

- Operator — умова активації правила. Наприклад, може бути встановлено на «equals», що означає «дорівнює».
- Value — конкретне значення для параметра, зазначеного в полі Field. Наприклад, це може бути конкретна IP-адреса, для якої потрібно встановити блокування.

Кнопки «And» та «Or», розташовані праворуч, дозволяють задавати додаткові умови для правила. Використання «And» означає, що правило активується, коли виконуються обидві умови, тоді як «Or» вказує на активацію правила при виконанні будь-якої з умов.

Для розширення області дії правила до діапазону IP-адрес, можна вибрати «And» та ввести наступні деталі:

- Field — знову вибір «IP address».
- Operator — «is in», що означає «входить в».
- Value — діапазон IP-адрес у форматі «IP-адреса/префікс CIDR».

Наприклад, можна ввести «2.16.64.0/24», що означає, що перші три сегменти IP-адреси (2.16.64) залишаються незмінними, а останній сегмент включає всі значення від 1 до 254. Якщо вказати «2.16.64.0/25», то останній сегмент буде включати значення від 1 до 126.

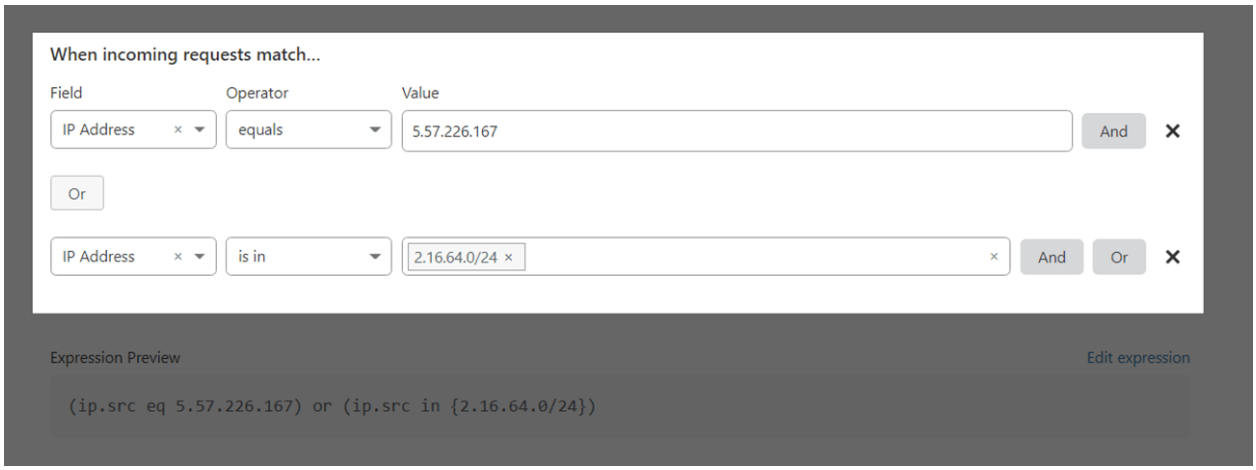

Рис.3.13. Розширення дії правила до діапазону IP-адрес

Під полями для деталізації правила знаходиться поле для визначення дії, яку Cloudflare застосує в разі, якщо запит відповідає визначеним умовам:

- Block — блокування доступу.
- Challenge (CAPTCHA) — відображення капчі. Використовується сервіс Google reCAPTCHA.
- JS Challenge — показ міжсторінкового повідомлення, аналогічно опції «I'm Under Attack!».
- Bypass — відключення перевірок Cloudflare.
- Allow — надання повного доступу.

У контексті наведеного прикладу, для блокування трафіку, вибирається опція «Block».

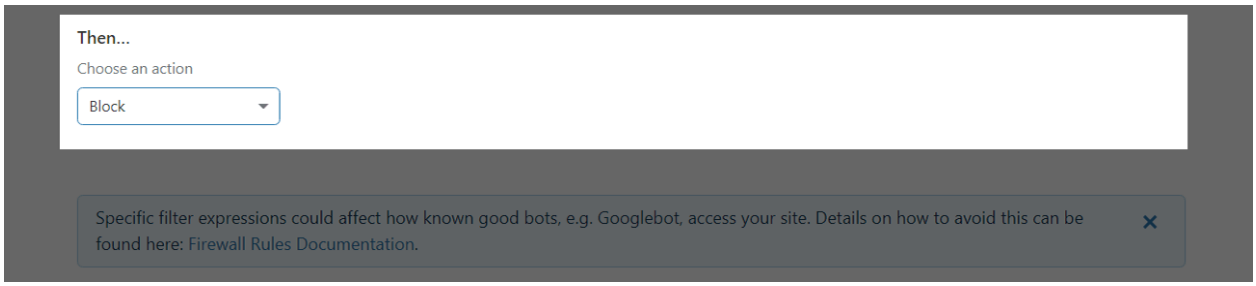

Рис.3.14 Опція «Block» для блокування трафіку

По завершенні налаштування правила, необхідно натиснути кнопку «Deploy», розташовану в нижній частині сторінки. Внесені зміни почнуть діяти негайно.

Для покращення роботи окремих сторінок можна створити специфічні правила, які регулюватимуть роботу певних компонентів Cloudflare для цих сторінок, або змінюватимуть їх функціонал.

У межах безкоштовного плану Cloudflare, користувачам надається можливість створити до трьох правил управління сторінками. Спочатку важливо розуміти загальний процес створення цих правил, після чого можна розглянути конкретні приклади правил, які можуть бути використані для специфічних потреб.

Процес створення правил розпочинається з доступу до інформаційної панелі Cloudflare. На панелі управління необхідно знайти розділ «Page Rules», де в першому блоку вибирається опція «Create Page Rule». Ця функція дозволяє користувачам створювати правила, які керують поведінкою певних сторінок або шаблонів URL на їх веб-сайті. Використання цих правил може включати перенаправлення трафіку, зміну налаштувань кешування, застосування налаштувань безпеки та багато іншого.

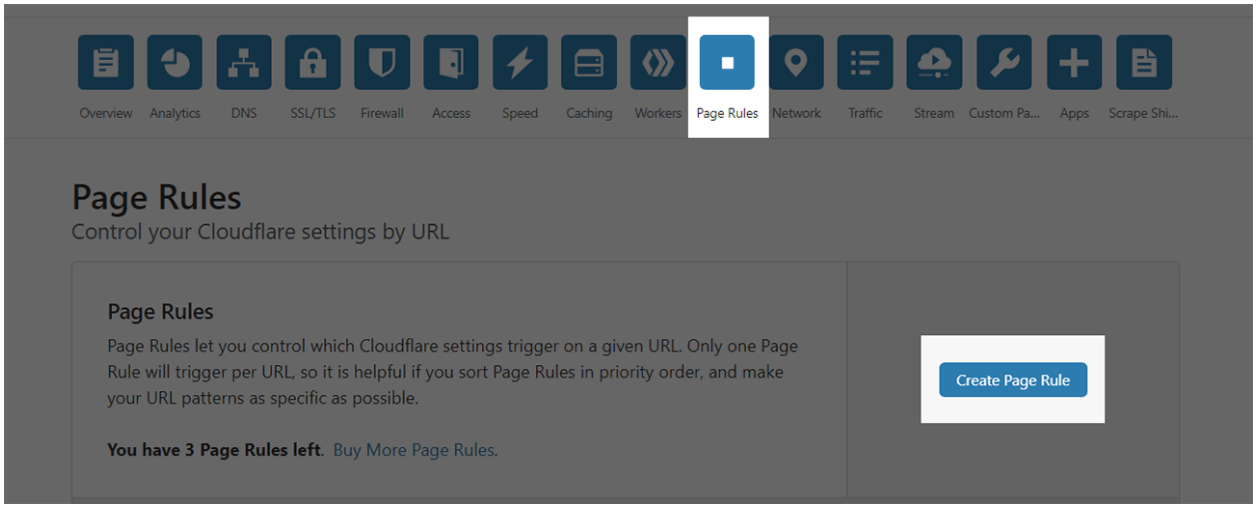

Рис.3.15. Створення правил

На наступному етапі створення правила для окремих сторінок можна зустріти два основних блоки з полями:

- **If the URL matches** — це поле для введення URL-адреси, до якої буде застосовуватися правило. Можна використовувати символ зірочки (*) у будь-якому сегменті URL-адреси, щоб перетворити його на шаблон. Наприклад, шаблон *.vashdomen.com/* буде означати, що правило діє на всі сторінки сайту, включаючи vashdomen.com, www.vashdomen.com/blog, shop.vashdomen.com/odezhda/muzhskoe і так далі.
- **Then the settings are** — це блок для вибору налаштувань, які будуть застосовуватися до зазначеного URL або шаблону. Якщо потрібно,

щоб для одного URL застосовувалося декілька налаштувань, можна додати їх, використовуючи кнопку «+ Add a Setting».

Після завершення налаштувань, правило потрібно зберегти та активувати, натиснувши кнопку «Save and Deploy».

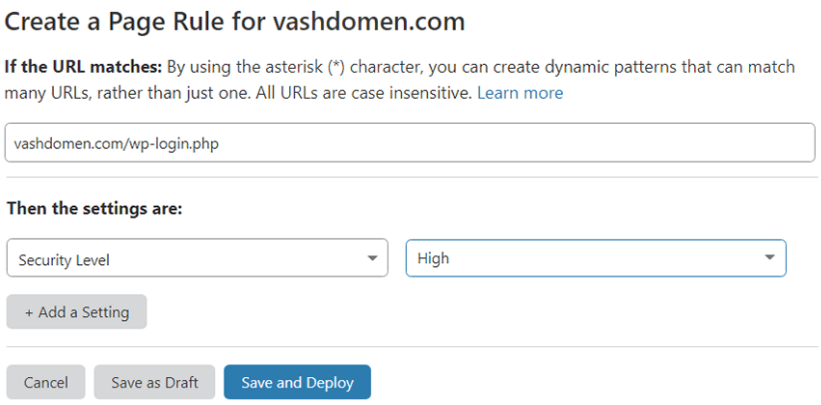

Рис.3.16. Створення правила для окремих сторінок

Черговість застосування правил залежить від їх розташування у списку. Щоб змінити порядок правил, користувачі можуть просто перетягнути потрібне правило вгору або вниз у списку, використовуючи значок для перетягування, який розташований зліва від правила.

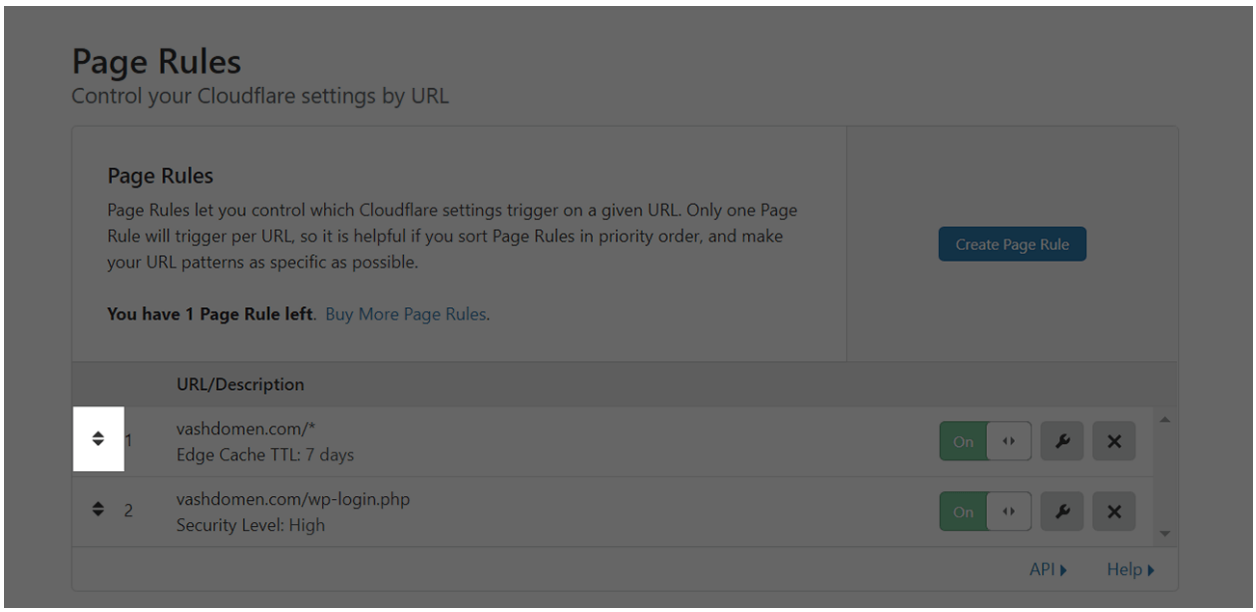

Рис.3.17. Зміна черговості застосування правил

Для забезпечення додаткового захисту сторінок авторизації, можна налаштувати спеціальні правила в Cloudflare, оскільки ці сторінки часто стають цілями хакерських атак. Їх можна створити в декілька етапів:

1. В полі **If the URL matches** необхідно вказати URL сторінки адміністративного доступу. Наприклад, для сайтів на WordPress це зазвичай адреса вигляду domain.com/wp-admin/*.

2. Далі, в полі **Then the settings are**, слід вибрати налаштування **Security Level – High**. Це збільшить ймовірність блокування доступу Cloudflare у разі підозрілої поведінки, наприклад, при тривалих та невдалих спробах доступу до акаунта.

3. Додатково можна використати опцію **+ Add a Setting** і обрати **Cache Level – Bypass**, щоб відключити кешування для цих сторінок. Це рекомендовано для сторінок авторизації, де кешування може бути небажаним.

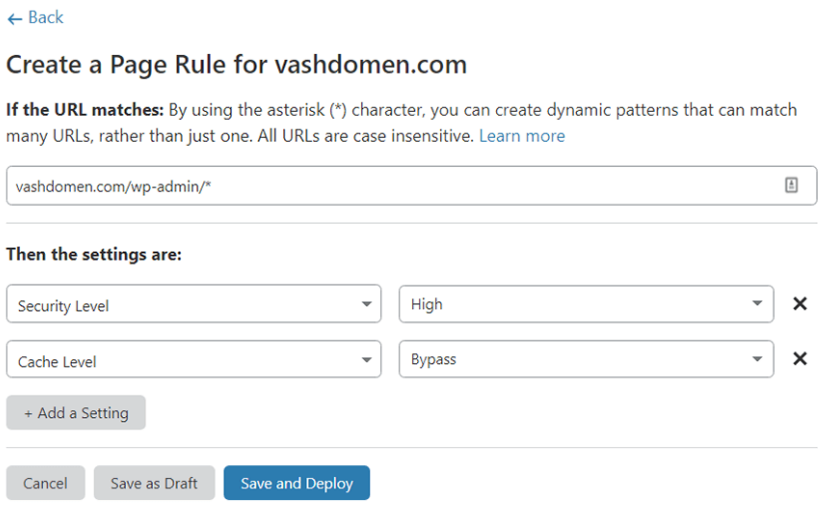

Рис.3.18. Налаштування спеціальних правил

Для контенту, який рідко змінюється, наприклад зображень, ефективне налаштування кешування може знизити навантаження на сервер та обсяг

використаного трафіку. Процес створення правила для такого контенту може включати наступні кроки:

1. В полі **If the URL matches**, вказати URL-адресу папки, де зберігаються зображення та інші мультимедійні файли.
2. В полі **Then the settings are**, обрати **Cache Level – Cache Everything** для того, щоб Cloudflare кешував увесь вміст цієї папки.
3. Використати опцію **+ Add a Setting** та додати **Browser Cache TTL – a day**, щоб кеш у браузерах відвідувачів оновлювався щодня.
4. Знову використати **+ Add a Setting** і додати **Edge Cache TTL – 7 days**, щоб Cloudflare оновлював кеш з файлами на стороні хостингу кожні 7 днів за потреби.

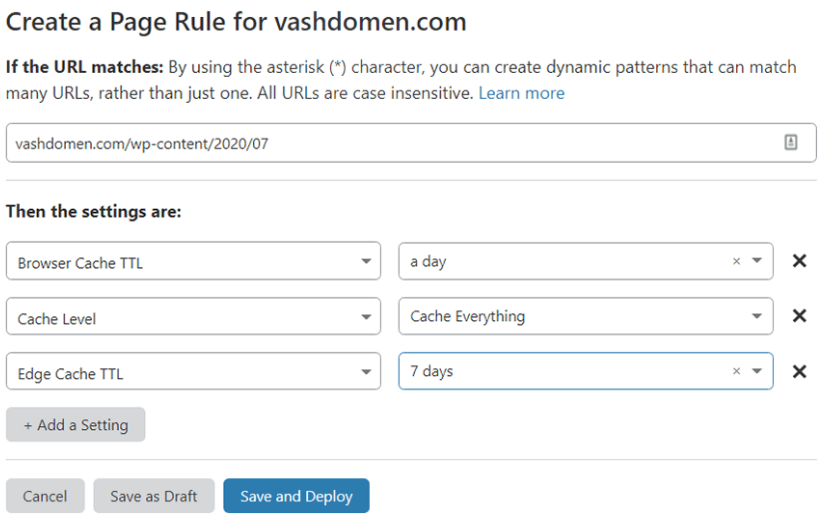

Рис.3.19. Створення правила для контенту, який рідко змінюється [12]

3.2. Налаштування правил протидії DDoS-атакам в інформаційній системі організації

Обробка помилкового спрацьовування

Обробка хибних спрацьовувань захисту від DDoS атак включає ідентифікацію та корекцію ситуацій, коли легітимний трафік неправильно класифікується як зловмисний. Це може виникати через використання

застарілих програм, проблемні інтернет-сервіси або клієнтські програми, які генерують законний трафік, але з відхиленнями від стандартних практик або порушеннями протоколів.

Системи захисту від DDoS-атак Cloudflare можуть помилково визначити такий трафік як зловмисний, застосовуючи заходи для його блокування. Якщо це відбувається з легальним трафіком, це може призвести до перебоїв у роботі сервісів.

Процедура виправлення хибних спрацьовувань включає такі кроки:

1. Увійти в інформаційну панель Cloudflare і вибрати відповідний обліковий запис.

2. Перейти до аналітичної панелі та застосувати відповідні фільтри:

- Для WAF/CDN клієнтів: вибрати зону, де відбуваються помилкові спрацьовування, перейти до розділу Безпека > Події, вибрати фільтр з параметром Сервіс дорівнює HTTP DDoS.
- Для клієнтів Magic Transit і Spectrum: перейти на сторінку Обліковий запис > Аналітика та журнали > Мережева аналітика, ідентифікувати легальний трафік, що спричиняє помилки.

3. Переглянути Топ подій за джерелом > HTTP DDoS правила, скопіювати назву правила.

4. Перейти до зони Безпека > DDoS, вибрати Розгорнути перевизначення DDoS.

5. Використати Огляд правил, знайти правило за назвою.

6. Зменшити рівень чутливості правила або змінити його дію на Журнал, якщо це можливо.

7. Натиснути Далі, потім Зберегти.

Після збереження правило набуде чинності протягом декількох хвилин. Коригування правил повинно забезпечити негайне рішення проблеми, що відображається в аналітичній панелі.

Додатково рекомендується увімкнути сповіщення про DDoS-атаки, щоб оперативно отримувати інформацію про потенційні атаки та можливі помилкові спрацьовування [13].

Обробка хибнонегативного результату або неповного усунення

Обробка помилкових негативних результатів або неповного усунення наслідків включає розгляд ситуацій, де DDoS-атаки неправильно ідентифікуються як легітимний трафік або коли застосовані заходи пом'якшення не забезпечують повного блокування атаки.

Помилкові Негативні Результати: При помилкових негативних результатах, трафік атаки іноді помилково класифікується як законний. Це може відбуватися, якщо атакуючий трафік недостатньо великий для активації заходів пом'якшення або відсутні специфічні правила для його ідентифікації.

Для усунення:

- Клієнтам WAF/CDN рекомендується виконувати кроки на сторінці "Реагування на DDoS-атаки", активувати режим "Під час атаки", створити правила обмеження швидкості та користувацькі правила WAF.
- Клієнтам Magic Transit слід використовувати правила Magic Firewall для пом'якшення наслідків атаки.

Неповне Усунення Наслідків: Неповне усунення наслідків виникає, коли заходи пом'якшення застосовані, але не забезпечують повного блокування атаки. Це може статися, якщо Cloudflare застосовує менш суворі заходи, ніж необхідно.

Коригування Правил:

1. Увійти в інформаційну панель Cloudflare та вибрати обліковий запис.
2. Перейти до аналітичної панелі, вибрати зону, де спостерігається неповне усунення наслідків для WAF/CDN клієнтів, або перейти в "Особистий кабінет > Аналітика та журнали > Мережева аналітика" для клієнтів Magic Transit та Spectrum.

3. Визначити атаку, використовуючи ідентифікатор атаки або фільтри.

4. Скопіювати назву правила, перейти до своєї зони > Безпека > DDoS.

5. Розгорнути перевизначення DDoS, вибрати Огляд правил та змінити дію правила на Блокувати.

6. Натиснути Далі та Зберегти.

Після збереження правило набуває чинності протягом декількох хвилин.

Альтернативна Процедура: У випадку неможливості зупинити атаку, що перевантажує вихідний веб-сервер, необхідно звернутися до служби підтримки Cloudflare з такою інформацією:

- Період часу атаки (UTC).
- Домен/шлях, який є ціллю атаки.
- Частота атак.
- Кроки для відтворення проблеми з фактичними та очікуваними результатами.
- Додаткова інформація, така як URL-адреси, повідомлення про помилки, скріншоти або журнали з вихідного веб-сервера [14].

3.3. Розроблення рекомендацій для захисту інформаційної системи організації від DDoS-атак

Підвищення стійкості сайту до DDoS-атак має вирішальне значення для забезпечення безперебійного обслуговування користувачів. Методи запобігання DDoS-атакам, які допоможуть захистити сайт від DDoS-атак і впоратися з піками трафіку:

1. Багаторівневий захист від DDoS-атак

DDoS-атаки вже не ті, що були 5-10 років тому. Раніше DDoS-атаки були переважно 3-го або 4-го рівня - об'ємні атаки, які атакували мережевий

або транспортний рівні. Сьогодні DDoS-атаки мають багато різних типів, і кожен тип націлений на окремий рівень (мережевий, транспортний, сеансовий, прикладний) або комбінацію рівнів.

Крім того, зловмисники знаходять нові способи зробити веб-сайти недоступними для легального трафіку та смертоносні методи використання вразливостей, організовуючи надзвичайно складні атаки.

Враховуючи цей контекст, DDoS-атакам неможливо запобігти простим збільшенням пропускної здатності мережі або використанням традиційних брандмауерів. Потрібне комплексне, багатомодульне та багаторівневе рішення для захисту від DDoS-атак, щоб уникнути всіх видів атак, включаючи DDoS-атаки на рівні додатків.

Отже, рішення повинно бути масштабованим і мати вбудовані можливості резервування, моніторингу трафіку, виявлення помилок бізнес-логіки та управління вразливостями.

2. Уникнення перетворення на бота

Однією з поширених тактик зловмисників є DDoS-ботнет - мережа скомпрометованих пристроїв, керованих віддалено для надсилання великого обсягу трафіку на ціль.

Наприклад, внутрішній веб-сайт користувача(або база даних, або будь-який інший подібний ресурс), який не є відкритим для громадськості, не працює через DDoS-атаку.

У чому підступ?

Жоден співробітник не стане атакувати актив своєї компанії. Отже, існує ймовірність того, що деякі системи співробітників скомпрометовані і використовуються як боти. Отже, працівники повинні бути навчені тому, як не бути використаними.

Щоб не стати ботом, можна зробити кілька речей:

- Оновлювати пристрої та програмне забезпечення;
- Використовувати надійні та унікальні паролі;

- Бути обережними з підозрілими електронними листами та вкладеннями;
- Використовувати надійне рішення для захисту від шкідливих програм;
- Використовувати надійний VPN.

3. Розпізнавання типів атак

Здатність визначати тип атаки раніше, ніж зловмисники, є невід'ємною частиною програми захисту від DDoS-атак. Існує три найпоширеніші типи DDoS-атак, з якими може зіткнутися компанія:

Рівень 7, рівень додатків або HTTP-затоплення

Цей тип атак на рівні додатків націлений на додаток, який отримує запити з декількох джерел. Такі атаки генерують великі обсяги POST, GET або HTTP-запитів, що призводить до простою сервісу від кількох годин до кількох тижнів. DDoS-атаки 7-го рівня широко використовуються для виведення з ладу веб-сайтів електронної комерції, банківської справи та стартапів через низьку вартість і простоту проведення.

Посилення UDP

Зловмисник перевантажує цільовий сервер або мережу відкритим трафіком NTP-запитів. Цей трафік на рівні 3 або 4 (мережевий або транспортний) посилюється трафіком корисного навантаження і є величезним порівняно з розміром запиту, а отже, перевантажує службу.

DNS-флуд

DNS-флуд - це DDoS-атака, спрямована на сервери DNS (Система доменних імен), які перетворюють доменні імена в IP-адреси. Ця атака спрямована на перевантаження DNS-серверів великим обсягом трафіку, що унеможливлює доступ легальних користувачів до цільового веб-сайту або онлайн-сервісу.

Розуміючи характеристики кожного типу атаки та швидко ідентифікуючи їх, програма захисту від DDoS може реагувати в режимі

реального часу, ефективно зменшуючи атаку до того, як вона завдасть значної шкоди.

Визначення типу атаки дозволяє застосовувати більш цілеспрямовані та ефективні механізми захисту, такі як фільтрація певного трафіку або блокування шкідливих IP-адрес. Крім того, рання ідентифікація типу атаки може допомогти передбачити і запобігти майбутнім атакам і поліпшити загальний стан безпеки.

4. Створення моделі загроз DDoS-атак

Модель загроз DDoS-атак - це структурований підхід до виявлення та аналізу потенційних ризиків для онлайн-сервісу або веб-сайту від DDoS-атак.

Більшість компаній нової ери борються з інвентаризацією веб-ресурсів, щоб не відставати від зростаючих темпів розвитку та вимог клієнтів. Нові клієнтські портали, платіжні шлюзи, системи додатків, маркетингові домени та інші ресурси часто створюються і видаляються. Варто визначити чи впорядковані веб-ресурси користувача:

- Визначити активи, які потрібно захистити - створити базу даних усіх веб-ресурсів, які потрібно захистити від DDoS-атак, у вигляді інвентаризаційного листа. Вона повинна містити інформацію про мережу, протоколи, що використовуються, домени, кількість додатків, їх використання, останню оновлену версію тощо.
- Визначити потенційних зловмисників - Далі потрібно визначити потенційних зловмисників, які можуть бути націлені на активи організації, наприклад, хактивістів, конкурентів або представників національних держав.
- Визначити вектори атаки - визначити різні вектори атаки, які зловмисник може використати для запуску DDoS-атаки, наприклад, UDP-флуд, SYN-флуд або HTTP-флуд.
- Визначити поверхню атаки - визначити поверхню атаки на активи організації, включаючи топологію мережі, апаратну інфраструктуру та стек програмного забезпечення.

- Оцінити рівень ризику - оцінити рівень ризику кожного вектора атаки, оцінивши ймовірність виникнення атаки, потенційний вплив атаки, а також ймовірність виявлення та пом'якшення наслідків атаки.

5. Встановлення пріоритетів для DDoS-атак

Початок процесу підвищення кіберзахисту включає в себе встановлення пріоритетів для веб-ресурсів організації, зокрема щодо їх важливості у контексті захисту від DDoS-атак. Важливо, щоб бізнес-активи та дані, що використовуються в веб-ресурсах, отримали найвищий пріоритет і були захищені цілодобово від DDoS-атак.

Визначення критичності веб-ресурсів:

- Критично важливі: В цю категорію слід включати активи, критичні для бізнес-транзакцій або впливаючі на репутацію компанії. Такі ресурси є пріоритетними цілями для хакерських атак.
- Високий пріоритет: До цього рівня відносяться веб-ресурси, котрі відіграють важливу роль у щоденній діяльності бізнесу і можуть бути вразливими до переривань.
- Нормальний пріоритет: До цієї категорії належать усі інші веб-ресурси, які не входять до вищеназваних груп.

Також рекомендується створити окрему категорію для доменів, мереж, додатків і інших сервісів, які більше не використовуються у бізнес-операціях. Їх необхідно відокремити від основної мережі, щоб мінімізувати потенційні ризики.

6. Зменшення поверхні, що піддається атаці

Скорочення доступної для потенційних зловмисників площі поверхні є критично важливим у стратегії мінімізації ризиків DDoS-атак. Ефективний захист інфраструктури, включаючи критичні активи, програми, ресурси, порти, протоколи та сервери, від несанкціонованого доступу, є ключовим кроком у цьому процесі. Для зниження вразливості можна використовувати різні стратегії:

1. Сегрегація та Розподіл Ресурсів: Розподіл ресурсів в мережі таким чином, щоб ускладнити їх атаку, наприклад, розміщення веб-серверів у публічній підмережі, а серверів баз даних - у приватній. Обмеження доступу до серверів баз даних з певних хостів.

2. Географічне Обмеження Трафіку: Застосування обмежень на доступ до сайтів з певних географічних регіонів, виходячи з розташування цільової аудиторії.

3. Використання Балансувальників Навантаження: Захист веб-серверів та обчислювальних ресурсів за допомогою балансувальників навантаження, які розташовані попереду цих компонентів.

4. Очищення Додатків/Сайтів: Видалення застарілих, непотрібних чи нерелевантних сервісів, функцій та процесів, які можуть бути використані зловмисниками як точки входу для атак.

7. Зміцнення мережевої архітектури

Один з ключових методів захисту від DDoS - зробити інфраструктуру та мережу здатними впоратися з будь-яким грозовим сплеском або раптовим стрибком трафіку. Як варіант, часто пропонують придбати додаткову пропускну здатність. Однак це не є практичним рішенням.

Підключення до послуги CDN допоможе використовувати глобальну розподілену мережу та створити надлишкові ресурси, здатні впоратися з раптовими об'ємними сплесками трафіку.

8. Розуміння попереджувальних знаків

DDoS-атаки мають певні ознаки. До найпоширеніших симптомів DDoS-атак відносяться нестабільне з'єднання в інтрамережі, періодичне вимкнення веб-сайтів та відключення інтернету. Однак проблема полягає в тому, що попереджувальні знаки схожі на інші проблеми, які можуть виникнути у системі організації, наприклад, віруси або повільне з'єднання з Інтернетом.

Якщо ці проблеми є більш серйозними і тривалими, мережа, швидше за все, зазнає DDoS-атаки, і потрібно вжити належних заходів для запобігання DDoS-атакам.

Ось деякі попереджувальні ознаки того, що на організацію може бути здійснена розподілена атака на відмову в обслуговуванні (DDoS):

- Незвично високий обсяг трафіку
- Повільна робота або відсутність реакції веб-сайту
- Проблеми з підключенням до мережі
- Незвичайні шаблони трафіку
- Неочікувані помилки сервера
- Незвичайні стрибки у використанні ресурсів

9. Обмеження швидкості

Обмеження швидкості - це метод, який використовується для запобігання розподіленим атакам на відмову в обслуговуванні (DDoS) шляхом обмеження обсягу трафіку, що надсилається до мережі або сервера. Це передбачає обмеження кількості запитів або з'єднань, які можуть бути здійснені протягом певного періоду часу.

Коли ліміт досягнуто, надлишковий трафік скидається або затримується. Обмеження швидкості може бути реалізовано на різних рівнях, наприклад, на рівні мережі, програми або DNS. Обмежуючи обсяг трафіку, який може бути надісланий до мережі або сервера, обмеження швидкості допомагає запобігти перевантаженню ресурсів, що може призвести до DDoS-атаки. Однак важливо ретельно налаштовувати обмеження швидкості, щоб уникнути блокування легітимного трафіку.

Такі заходи, як обмеження географічного доступу, обмеження доступу на основі оцінок репутації тощо, що базуються на інформації в режимі реального часу, мають велике значення для запобігання DDoS-атакам.

10. Моніторинг та аналіз логів

Зупинка DDoS-атак через моніторинг логів є одним із ключових підходів до захисту від цих загроз. Ця практика включає швидке виявлення потенційних атак за допомогою аналізу даних і статистики веб-трафіку, зафіксованих у файлах журналів. Ці файли містять важливу інформацію, яка дозволяє ідентифікувати аномалії в реальному часі.

Інструменти для аналізу логів не тільки допомагають виявляти DDoS-загрози, але й пропонують переваги, такі як швидке виявлення та спрощений процес відновлення після атак. Журнали дозволяють відстежувати статистику трафіку, включаючи час і масштаб сплесків активності, а також вказують, які сервери були залучені в атаку.

Використання аналізу логів сприяє економії часу, оскільки воно дозволяє швидше ідентифікувати та усувати проблеми, попереджаючи про можливі неполадки. Деякі розширені інструменти управління журналами навіть забезпечують інформацію, необхідну для ефективного відновлення після успішної DDoS-атаки.

11. Підготовка план стійкості до DDoS-атак

Бізнес має усвідомлювати, що стратегія захисту від DDoS-атак не обмежується тільки їх запобіганням та зменшенням їх впливу. Враховуючи, що метою DDoS-атаки є повна зупинка діяльності компанії, більшість захисних заходів зосереджені на її припиненні. Важливою складовою є планування та впровадження процедур аварійного відновлення як частини звичайного процесу обслуговування.

План аварійного відновлення повинен базуватися на технічній компетенції та включати детальний комплексний план. Цей план має описувати, як підтримувати безперервність бізнес-процесів під час та після успішної DDoS-атаки.

Сайт аварійного відновлення є ключовою частиною плану стійкості бізнесу. Цей сайт, що слугує тимчасовою альтернативою основному майданчику, повинен містити актуальні резервні копії даних. План відновлення також має включати такі важливі аспекти, як методи

відновлення, місця зберігання резервних копій критичних даних та визначення відповідальних за виконання специфічних завдань.

12. Отримання інструментів захисту від DDoS-атак

На сучасному ринку представлено чимало інструментів, які допомагають виявляти та мінімізувати ризики від DDoS-атак, що впливають на критичні веб-ресурси. Ці інструменти можна класифікувати за двома основними напрямками: виявлення та пом'якшення наслідків атак.

Виявлення: Ефективність пом'якшення наслідків DDoS-атак значною мірою залежить від здатності вчасно виявляти неавтентичні сплески трафіку, перш ніж вони завдають суттєвої шкоди. Багато інструментів для захисту від DDoS-атак використовують сигнатури та дані про джерела для попередження про потенційні загрози. Вони чекають, коли трафік досягне критичного рівня, який може вплинути на доступність сервісів. Проте, наявність тільки виявлення недостатня, оскільки часто потрібне ручне втручання для аналізу даних і застосування захисних правил.

Автоматизоване Усунення Наслідків: Чи можлива автоматизація захисту від DDoS? Чимало рішень у цій сфері включають напрямки, які автоматично блокують або перенаправляють шкідливий трафік на основі заздалегідь встановлених правил і політик. Автоматична фільтрація небажаного трафіку на рівнях додатків або мережі є бажаною опцією, але зловмисники постійно розробляють нові способи обходу цих захисних заходів, особливо на рівні додатків.

13Традиційні брандмауери

Незважаючи на те, що традиційні брандмауери стверджують, що мають вбудовані функції захисту від DDoS, вони мають лише один метод блокування DDoS - практику невибіркових порогових значень, яка блокує певний порт, коли досягається його максимальне порогове значення.

Кіберзлочинці знають, що це ідеальний спосіб блокувати як законних, так і зловмисних користувачів. Кінцева мета досягається, оскільки це впливає на роботу програми та доступність мережі.

14. Розгортання брандмауера веб-додатків

Брандмауер веб-додатків (WAF) є важливим інструментом у захисті від DDoS-атак, оскільки він зосереджений на блокуванні шкідливого трафіку та захисті вразливостей самого додатку. Системи, подібні до AppTrana, забезпечують захист від DDoS-атак через цілодобовий моніторинг від фахівців з безпеки. Це дозволяє виявляти та блокувати неавтентичні сплески трафіку, не заважаючи легітимному трафіку.

WAF може бути розміщений між інтернетом та сервером джерела, діючи як зворотний проксі. Він захищає сервер, змушуючи весь трафік проходити через WAF перед тим, як потрапити на сервер. Використання WAF дає змогу швидко реалізовувати користувацькі правила у відповідь на атаки, ефективно відсікаючи шкідливий трафік до того, як він досягне сервера, тим самим зменшуючи навантаження.

Залежно від конкретних потреб та інфраструктури, WAF може бути реалізований у трьох різних формах:

1. WAF на основі мережі: Це фізичні або віртуальні пристрої, розміщені у мережевій інфраструктурі.
2. WAF на базі хоста: Встановлюється безпосередньо на сервер, де розміщений веб-додаток.
3. Хмарний WAF: Це хмарні рішення, які забезпечують гнучкість та масштабованість захисту без необхідності встановлення фізичного обладнання.

Ідеальна комбінація: WAF і захист від DDoS-атак

Важливою складовою стратегії захисту від DDoS-атак є ретельне відстеження вхідного трафіку. Регулярно оновлювані журнали трафіку забезпечують інформацію про обмін даними в програмі або мережі, дозволяючи виявляти аномалії. Неперервний моніторинг і аналіз допомагають організаціям навчатися на основі історичних даних про атаки та визначати шаблони загроз. Централізований моніторинг стає ключовим на

рівні додатків, де команди кібербезпеки можуть відстежувати аномалії, сигнатури бот-мереж і підозрілу поведінку.

Поведінковий аналіз, який є частиною WAF, безперервно моніторить і записує поведінку користувачів та організацій, виявляючи аномалії, що не відповідають звичним шаблонам. Використовуючи розширений аналіз, журнали, звіти та дані про загрози, такий метод точно ідентифікує потенційних зловмисників.

Хмарні рішення для захисту від DDoS-атак забезпечують додаткові можливості фільтрації, переважаючи над традиційними брандмауерами. Хмарні WAF надають віртуальну масштабованість і не обмежені пропускною спроможністю. Вони також є керованими послугами, які не вимагають додаткових інвестицій в обслуговування, забезпечуючи ефективний захист як на рівні додатків, так і на мережевому рівні.

Крім того, хмарний захист від DDoS здатний зупиняти атаки мережевого рівня, такі як UDP-флуди та SYN-флуди, а також атаки на рівні додатків, включаючи TCP-з'єднання, DNS-флуд, HTTP-флуд і низькошвидкісні атаки.

Стрічка розвідки загроз надає інформацію про відомі та нові загрози, включаючи дані про минулі DDoS-атаки, що дозволяє постійно налаштовувати рішення для захисту.

WAF, які використовують алгоритми машинного навчання, здатні виявляти та блокувати складніші атаки, вчачись і адаптуючись до нових шаблонів загроз. Вони також можуть ідентифікувати DDoS-атаки на додатки, навіть коли корисне навантаження виглядає легітимним. Використання користувацьких політик дозволяє відрізняти звичайні людські транзакції від автоматизованих, підвищуючи ефективність боротьби з DDoS-атаками на рівні додатків [15].

ВИСНОВОК

Розподілені атаки типу "відмова в обслуговуванні" (DDoS) представляють собою одну з найбільш серйозних загроз для підприємств та організацій у сучасному Інтернет-просторі. Хакери, які виконують ці атаки, перевантажують мережі величезним обсягом трафіку, що перевищує їхні можливості, роблячи мережі недоступними для легітимних користувачів.

Наслідки DDoS-атак можуть бути руйнівними для бізнесу, включаючи значні фінансові втрати, падіння довіри клієнтів та погіршення репутації. Окрім безпосереднього впливу на доступність послуг, DDoS-атаки часто використовуються як відволікаючий маневр для інших зловмисних дій, таких як крадіжка даних або розповсюдження шкідливого програмного забезпечення.

З огляду на ці ризики, для компаній є життєво важливим розробити та впровадити ефективні стратегії захисту від DDoS-атак. Це включає в себе не лише технічні засоби, такі як вдосконалені системи виявлення та пом'якшення наслідків атак, але й організаційні заходи, наприклад, регулярний аудит безпеки та підготовка персоналу.

Важливим є також постійне спостереження та аналіз мережевого трафіку, щоб адміністратори могли швидко реагувати на будь-які ознаки атаки. Проактивний підхід до кібербезпеки та оперативне реагування на інциденти є ключовими факторами в захисті організацій від сучасних кіберзагроз.

ПЕРЕЛІК ПОСИЛАНЬ

1. Why is a DDoS attack dangerous?. *NETSCOUT*. URL: https://www.netscout.com/what-is-ddos/why-is-ddos-dangerous#:~:text=What%20are%20the%20consequences%20of,productivity%20grind%20to%20a%20halt. (дата звернення: 11.11.2023).
2. What is a DDoS botnet?. *Cloudflare*. URL: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-botnet/ (дата звернення: 11.11.2023).
3. What is a DDoS attack?. *Cloudflare*. URL: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ (дата звернення: 11.11.2023).
4. What is a DDOS Attack & How to Protect Your Site Against One. *Amazon Web Services, Inc.* URL: https://aws.amazon.com/shield/ddos-attack-protection/?nc1=h_ls (дата звернення: 14.11.2023).
5. 9 Best DDoS Protection Service Providers for 2024. *eSecurity Planet*. URL: https://www.esecurityplanet.com/products/distributed-denial-of-service-ddos-protection-vendors/ (дата звернення: 14.11.2023).
6. Cloudflare DDoS Protection · Cloudflare DDoS Protection docs. *Home · Cloudflare Docs*. URL: https://developers.cloudflare.com/ddos-protection/ (дата звернення: 15.11.2023).
7. How DDoS protection works · Cloudflare DDoS Protection docs. *Home · Cloudflare Docs*. URL: https://developers.cloudflare.com/ddos-protection/about/how-ddos-protection-works/#:~:text=To%20detect%20and%20mitigate%20DDoS,causing%20latency%20or%20impacting%20performance. (дата звернення: 15.11.2023).
8. Managed rulesets · Cloudflare DDoS Protection docs. *Home · Cloudflare Docs*. URL: https://developers.cloudflare.com/ddos-protection/managed-rulesets/ (дата звернення: 18.11.2023).

9. Adaptive DDoS Protection · Cloudflare DDoS Protection docs. *Home · Cloudflare Docs*. URL: https://developers.cloudflare.com/ddos-protection/managed-rulesets/adaptive-protection/ (дата звернення: 25.11.2023).

10. Cloudflare Advanced TCP Protection · Cloudflare DDoS Protection docs. *Home · Cloudflare Docs*. URL: https://developers.cloudflare.com/ddos-protection/tcp-protection/ (дата звернення: 08.12.2023).

11. Advanced DNS Protection (beta) · Cloudflare DDoS Protection docs. *Home · Cloudflare Docs*. URL: https://developers.cloudflare.com/ddos-protection/dns-protection/ (дата звернення: 08.12.2023).

12. Cloudflare – що це і як налаштувати | HOSTiQ Wiki. *HOSTiQ Wiki*. URL: https://hostiq.ua/wiki/ukr/dns-hosting-cloudflare/ (дата звернення: 12.12.2023).

13. Handle a false positive · Cloudflare DDoS Protection docs. *Home · Cloudflare Docs*. URL: https://developers.cloudflare.com/ddos-protection/managed-rulesets/adjust-rules/false-positive/ (дата звернення: 12.12.2023).

14. Handle a false negative or an incomplete mitigation · Cloudflare DDoS Protection docs. *Home · Cloudflare Docs*. URL: https://developers.cloudflare.com/ddos-protection/managed-rulesets/adjust-rules/false-negative/ (дата звернення: 15.12.2023).

15. 15 Best Practices for DDoS Protection | Indusface Blog. *Indusface*. URL: https://www.indusface.com/blog/best-practices-to-prevent-ddos-attacks/ (дата звернення: 19.12.2023).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)